[Reserved]

Incentive compensation practices in the financial industry were one of many factors that contributed to the financial crisis that began in mid-2007. Banking organizations too often rewarded employees for increasing the organization's revenue or short-term profit without adequate recognition of the risks the employees' activities posed to the organization.[1] These practices exacerbated the risks and losses at a number of banking organizations and resulted in the misalignment of the interests of employees with the long-term well-being and safety and soundness of their organizations. This section provides guidance on sound incentive compensation practices to banking organizations supervised by the Federal Reserve (also the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision (collectively, the "Agencies")).[2] This guidance is intended to assist banking organizations in designing and implementing incentive compensation arrangements and related policies and procedures that effectively consider potential risks and risk outcomes.[3]

Alignment of incentives provided to employees with the interests of shareholders of the organization often also benefits safety and soundness. However, aligning employee incentives with the interests of shareholders is not always sufficient to address safety-and-soundness concerns. Because of the presence of the federal safety net (including the ability of insured depository institutions to raise insured deposits and access the discount window and payment services of the Federal Reserve), shareholders of a banking organization in some cases may be willing to tolerate a degree of risk that is inconsistent with the organization's safety and soundness. Accordingly, the Federal Reserve expects banking organizations to maintain incentive compensation practices that are consistent with safety and soundness, even when these practices go beyond those needed to align shareholder and employee interests.

To be consistent with safety and soundness, incentive compensation arrangements[4] at a banking organization should:

1. Provide employees incentives that appropriately balance risk and reward;
2. Be compatible with effective controls and risk-management; and
3. Be supported by strong corporate governance, including active and effective oversight by the organization's board of directors.

These principles, and the types of policies, procedures, and systems that banking organizations should have to help ensure compliance with them, are discussed later in this guidance.

The Federal Reserve expects banking organizations to regularly review their incentive compensation arrangements for all executive and non-executive employees who, either individually or as part of a group, have the ability to expose the organization to material amounts of risk, as well as to regularly review the risk-management, control, and corporate governance processes related to these arrangements. Banking organizations should immediately address any identified deficiencies in these arrangements or processes that are inconsistent with safety and soundness. Banking organizations are responsible for ensuring that their incentive compensation arrangements are consistent with the prin-

1. Examples of risks that may present a threat to the organization's safety and soundness include credit, market, liquidity, operational, legal, compliance, and reputational risks.

2. As used in this guidance, the term "banking organization" includes national banks, state member banks, state nonmember banks, savings associations, U.S. bank holding companies, savings and loan holding companies, Edge and agreement corporations, and the U.S. operations of foreign banking organizations (FBOs) with a branch, agency, or commercial lending company in the United States. If the Federal Reserve is referenced, the reference is intended to also include the other supervisory Agencies.

3. This guidance (see 75 *Fed. Reg.* 36395, June 25, 2010, for the entire text) and the principles reflected herein are consistent with the *Principles for Sound Compensation Practices* issued by the Financial Stability Board (FSB) in April 2009, and with the FSB's *Implementation Standards* for those principles, issued in September 2009.

4. In this guidance, the term "incentive compensation" refers to that portion of an employee's current or potential compensation that is tied to achievement of one or more specific metrics (e.g., a level of sales, revenue, or income). Incentive compensation does not include compensation that is awarded solely for, and the payment of which is solely tied to, continued employment (e.g., salary). In addition, the term does not include compensation arrangements that are determined based solely on the employee's level of compensation and does not vary based on one or more performance metrics (e.g., a 401(k) plan under which the organization contributes a set percentage of an employee's salary).

ciples described in this guidance and that they do not encourage employees to expose the organization to imprudent risks that may pose a threat to the safety and soundness of the organization.

The Federal Reserve recognizes that incentive compensation arrangements often seek to serve several important and worthy objectives. For example, incentive compensation arrangements may be used to help attract skilled staff, induce better organization-wide and employee performance, promote employee retention, provide retirement security to employees, or allow compensation expenses to vary with revenue on an organization-wide basis. Moreover, the analysis and methods for ensuring that incentive compensation arrangements take appropriate account of risk should be tailored to the size, complexity, business strategy, and risk tolerance of each organization. The resources required will depend upon the complexity of the firm and its use of incentive compensation arrangements. For some, the task of designing and implementing compensation arrangements that properly offer incentives for executive and non-executive employees to pursue the organization's long-term well-being and that do not encourage imprudent risk-taking is a complex task that will require the commitment of adequate resources.

While issues related to designing and implementing incentive compensation arrangements are complex, the Federal Reserve is committed to ensuring that banking organizations move forward in incorporating the principles described in this guidance into their incentive compensation practices.[5]

As discussed further below, because of the size and complexity of their operations, large complex banking organizations (LCBOs)[6] should have and adhere to systematic and formalized policies, procedures, and processes. These are considered important in ensuring that incentive compensation arrangements for all covered employees are identified and reviewed by appropriate levels of management (including the board of directors where appropriate and control units), and that they appropriately balance risks and rewards. In several places, this guidance specifically highlights the types of policies, procedures, and systems that LCBOs should have and maintain but that generally are not expected of smaller, less complex organizations. LCBOs warrant the most intensive supervisory attention because they are significant users of incentive compensation arrangements and because flawed approaches at these organizations are more likely to have adverse effects on the broader financial system. The Federal Reserve will work with LCBOs as necessary through the supervisory process to ensure that they promptly correct any deficiencies that may be inconsistent with the safety and soundness of the organization.

The policies, procedures, and systems of smaller banking organizations that use incentive compensation arrangements[7] are expected to be less extensive, formalized, and detailed than those of LCBOs. Supervisory reviews of incentive compensation arrangements at smaller, less-complex banking organizations will be conducted by the Federal Reserve as part of the evaluation of those organizations' risk-management, internal controls, and corporate governance during the regular, risk-focused examination process. These reviews will be tailored to reflect the scope and complexity of an organization's activities, as well as the prevalence and scope of its incentive compensation arrangements. Little, if any, additional examination work is expected for smaller banking organizations that do not use, to a significant extent, incentive compensation arrangements.[8]

5. In December 2009, the Federal Reserve, working with the other Agencies, initiated a special horizontal review of incentive compensation arrangements and related risk-management, control, and corporate governance practices of large banking organizations (LBOs). This initiative was designed to spur and monitor the industry's progress towards the implementation of safe and sound incentive compensation arrangements, identify emerging best practices, and advance the state of practice more generally in the industry.

6. For supervisory purposes, the Federal Reserve (as well as the other federal bank regulatory agencies) segments the organizations it supervises into different supervisory portfolios based on, among other things, size, complexity, and risk profile. For purposes of this guidance, the LBOs referred to in the guidance are identified in this section as large complex banking organizations to be consistent with the Federal Reserve's other supervisory policies. LBOs are designated by (1) the OCC as the largest and most complex national banks as defined in the Large Bank Supervision booklet of the Comptroller's Handbook; (2) the FDIC, large, complex insured depository institutions (IDIs); and (3) the OTS, the largest and most complex savings associations and savings and loan holding companies.

7. This guidance does not apply to banking organizations that do not use incentive compensation.

8. To facilitate these reviews, where appropriate, a smaller banking organization should review its compensation arrangements to determine whether it uses incentive compensation arrangements to a significant extent in its business operations. A smaller banking organization will not be considered a significant user of incentive compensation arrangements simply because the organization has a firm-wide profit-sharing or

For all banking organizations, supervisory findings related to incentive compensation will be communicated to the organization and included in the relevant report of examination or inspection. In addition, these findings will be incorporated, as appropriate, into the organization's rating component(s) and subcomponent(s) relating to risk-management, internal controls, and corporate governance under the relevant supervisory rating system, as well as the organization's overall supervisory rating.

The Federal Reserve (or the organization's appropriate federal supervisor) may take enforcement action against a banking organization if its incentive compensation arrangements or related risk-management, control, or governance processes pose a risk to the safety and soundness of the organization, particularly when the organization is not taking prompt and effective measures to correct the deficiencies. For example, the appropriate federal supervisor may take an enforcement action if material deficiencies are found to exist in the organization's incentive compensation arrangements or related risk-management, control, or governance processes, or the organization fails to promptly develop, submit, or adhere to an effective plan designed to ensure that its incentive compensation arrangements do not encourage imprudent risk-taking and are consistent with principles of safety and soundness. As provided under section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), an enforcement action may, among other things, require an organization to take affirmative action, such as developing a corrective action plan that is acceptable to the appropriate federal supervisor to rectify safety-and-soundness deficiencies in its incentive compensation arrangements or related processes. Where warranted, the appropriate federal supervisor may require the organization to take additional affirmative action to correct or remedy deficiencies related to the organization's incentive compensation practices.

Effective and balanced incentive compensation practices are likely to evolve significantly in the coming years, spurred by the efforts of banking organizations, supervisors, and other stakeholders. The Federal Reserve will review and update this guidance as appropriate to incorporate best practices that emerge from these efforts.

bonus plan that is based on the bank's profitability, even if the plan covers all or most of the organization's employees.

SCOPE OF APPLICATION

The incentive compensation arrangements and related policies and procedures of banking organizations should be consistent with principles of safety and soundness.[9] Incentive compensation arrangements for executive officers as well as for non-executive personnel who have the ability to expose a banking organization to material amounts of risk may, if not properly structured, pose a threat to the organization's safety and soundness. Accordingly, this guidance applies to incentive compensation arrangements for:

1. Senior executives and others who are responsible for oversight of the organization's firm-wide activities or material business lines;[10]
2. Individual employees, including non-executive employees, whose activities may expose the organization to material amounts of risk (e.g., traders with large position limits relative to the organization's overall risk tolerance); and
3. Groups of employees who are subject to the same or similar incentive compensation arrangements and who, in the aggregate, may expose the organization to material amounts of risk, even if no individual employee is likely to expose the organization to material risk (e.g., loan officers who, as a group, originate loans that account for a material amount of the organization's credit risk).

For ease of reference, these executive and non-executive employees are collectively referred to hereafter as "covered employees" or "employees." Depending on the facts and circumstances of the individual organization, the

9. In the case of the U.S. operations of FBOs, the organization's policies, including management, review, and approval requirements for its U.S. operations, should be coordinated with the FBO's group-wide policies developed in accordance with the rules of the FBO's home country supervisor. The policies of the FBO's U.S. operations should also be consistent with the FBO's overall corporate and management structure, as well as its framework for risk-management and internal controls. In addition, the policies for the U.S. operations of FBOs should be consistent with this guidance.

10. Senior executives include, at a minimum, "executive officers" within the meaning of the Federal Reserve's Regulation O (see 12 CFR 215.2(e)(1)) and, for publicly traded companies, "named officers" within the meaning of the Securities and Exchange Commission's rules on disclosure of executive compensation (see 17 CFR 229.402(a)(3)). Savings associations should also refer to the OTS's rule on loans by savings associations to their executive officers, directors, and principal shareholders. (12 CFR 563.43).

types of employees or categories of employees that are outside the scope of this guidance because they do not have the ability to expose the organization to material risks would likely include, for example, tellers, bookkeepers, couriers, or data processing personnel.

In determining whether an employee, or group of employees, may expose a banking organization to material risk, the organization should consider the full range of inherent risks arising from, or generated by, the employee's activities, even if the organization uses risk-management processes or controls to limit the risks such activities ultimately may pose to the organization. Moreover, risks should be considered to be material for purposes of this guidance if they are material to the organization, or are material to a business line or operating unit that is itself material to the organization.[11]

For purposes of illustration, assume that a banking organization has a structured-finance unit that is material to the organization. A group of employees within that unit who originate structured-finance transactions that may expose the unit to material risks should be considered "covered employees" for purposes of this guidance even if those transactions must be approved by an independent risk function prior to consummation, or the organization uses other processes or methods to limit the risk that such transactions may present to the organization.

Strong and effective risk-management and internal control functions are critical to the safety and soundness of banking organizations. However, irrespective of the quality of these functions, poorly designed or managed incentive compensation arrangements can themselves be a source of risk to a banking organization. For example, incentive compensation arrangements that provide employees strong incentives to increase the organization's short-term revenues or profits, without regard to the short- or long-term risk associated with such business, can place substantial strain on the risk-management and internal control functions of even well-managed organizations.

Moreover, poorly balanced incentive compensation arrangements can encourage employees to take affirmative actions to weaken or circumvent the organization's risk-management or internal control functions, such as by providing inaccurate or incomplete information to these functions, to boost the employee's personal compensation. Accordingly, sound compensation practices are an integral part of strong risk-management and internal control functions. A key goal of this guidance is to encourage banking organizations to incorporate the risks related to incentive compensation into their broader risk-management framework. Risk-management procedures and risk controls that ordinarily limit risk-taking do not obviate the need for incentive compensation arrangements to properly balance risk-taking incentives.

PRINCIPLES OF A SOUND INCENTIVE COMPENSATION SYSTEM

Principle 1: Balanced Risk-Taking Incentives

Incentive compensation arrangements should balance risk and financial results in a manner that does not encourage employees to expose their organizations to imprudent risks.

Incentive compensation arrangements typically attempt to encourage actions that result in greater revenue or profit for the organization. However, short-run revenue or profit can often diverge sharply from actual long-run profit because risk outcomes may become clear only over time. Activities that carry higher risk typically yield higher short-term revenue, and an employee who is given incentives to increase short-term revenue or profit, without regard to risk, will naturally be attracted to opportunities to expose the organization to more risk.

An incentive compensation arrangement is balanced when the amounts paid to an employee appropriately take into account the risks (including compliance risks), as well as the financial benefits, from the employee's activities and the impact of those activities on the organization's safety and soundness. As an example, under a balanced incentive compensation arrangement, two employees who generate the same amount of short-term revenue or profit for an organization should not receive the same amount of incentive compensation if the risks taken by the employees in generating that revenue or profit differ materially. The employee whose activities create materially larger risks for the organiza-

11. Thus, risks may be material to an organization even if they are not large enough themselves to threaten the solvency of the organization.

tion should receive less than the other employee, all else being equal.

The performance measures used in an incentive compensation arrangement have an important effect on the incentives provided employees and, thus, the potential for the arrangement to encourage imprudent risk-taking. For example, if an employee's incentive compensation payments are closely tied to short-term revenue or profit of business generated by the employee, without any adjustments for the risks associated with the business generated, the potential for the arrangement to encourage imprudent risk-taking may be quite strong. Similarly, traders who work with positions that close at year-end could have an incentive to take large risks toward the end of a year if there is no mechanism for factoring how such positions perform over a longer period of time. The same result could ensue if the performance measures themselves lack integrity or can be manipulated inappropriately by the employees receiving incentive compensation.

On the other hand, if an employee's incentive compensation payments are determined based on performance measures that are only distantly linked to the employee's activities (e.g., for most employees, organization-wide profit), the potential for the arrangement to encourage the employee to take imprudent risks on behalf of the organization may be weak. For this reason, plans that provide for awards based solely on overall organization-wide performance are unlikely to provide employees, other than senior executives and individuals who have the ability to materially affect the organization's overall risk profile, with unbalanced risk-taking incentives.

Incentive compensation arrangements should not only be balanced in design, they also should be implemented so that actual payments vary based on risks or risk outcomes. If, for example, employees are paid substantially all of their potential incentive compensation even when risk or risk outcomes are materially worse than expected, employees have less incentive to avoid activities with substantial risk.

- *Banking organizations should consider the full range of risks associated with an employee's activities, as well as the time horizon over which those risks may be realized, in assessing whether incentive compensation arrangements are balanced.*

The activities of employees may create a wide range of risks for a banking organization, such as credit, market, liquidity, operational, legal, compliance, and reputational risks, as well as other risks to the viability or operation of the organization. Some of these risks may be realized in the short term, while others may become apparent only over the long term. For example, future revenues that are booked as current income may not materialize, and short-term profit-and-loss measures may not appropriately reflect differences in the risks associated with the revenue derived from different activities (e.g., the higher credit or compliance risk associated with subprime loans versus prime loans).[12] In addition, some risks (or combinations of risky strategies and positions) may have a low probability of being realized, but would have highly adverse effects on the organization if they were to be realized ("bad tail risks"). While shareholders may have less incentive to guard against bad tail risks because of the infrequency of their realization and the existence of the federal safety net, these risks warrant special attention for safety-and-soundness reasons given the threat they pose to the organization's solvency and the federal safety net.

Banking organizations should consider the full range of current and potential risks associated with the activities of covered employees, including the cost and amount of capital and liquidity needed to support those risks, in developing balanced incentive compensation arrangements. Reliable quantitative measures of risk and risk outcomes ("quantitative measures"), where available, may be particularly useful in developing balanced compensation arrangements and in assessing the extent to which arrangements are properly balanced. However, reliable quantitative measures may not be available for all types of risk or for all activities, and their utility for use in compensation arrangements varies across business lines and employees. The absence of reliable quantitative measures for certain types of risks or outcomes does not mean that banking organizations should ignore such risks or outcomes for purposes of assessing whether an incentive compensation

12. Importantly, the time horizon over which a risk outcome may be realized is not necessarily the same as the stated maturity of an exposure. For example, the ongoing reinvestment of funds by a cash management unit in commercial paper with a one-day maturity not only exposes the organization to one-day credit risk, but also exposes the organization to liquidity risk that may be realized only infrequently.

arrangement achieves balance. For example, while reliable quantitative measures may not exist for many bad-tail risks, it is important that such risks be considered given their potential effect on safety and soundness. As in other risk-management areas, banking organizations should rely on informed judgments, supported by available data, to estimate risks and risk outcomes in the absence of reliable quantitative risk measures.

Large complex banking organizations. In designing and modifying incentive compensation arrangements, LCBOs should assess in advance of implementation whether such arrangements are likely to provide balanced risk-taking incentives. Simulation analysis of incentive compensation arrangements is one way of doing so. Such analysis uses forward-looking projections of incentive compensation awards and payments based on a range of performance levels, risk outcomes, and levels of risks taken. This type of analysis, or other analysis that results in assessments of likely effectiveness, can help an LCBO assess whether incentive compensation awards and payments to an employee are likely to be reduced appropriately as the risks to the organization from the employee's activities increase.

- *An unbalanced arrangement can be moved toward balance by adding or modifying features that cause the amounts ultimately received by employees to appropriately reflect risk and risk outcomes.*

If an incentive compensation arrangement may encourage employees to expose their banking organization to imprudent risks, the organization should modify the arrangement as needed to ensure that it is consistent with safety and soundness. Four methods are often used to make compensation more sensitive to risk. These methods are:

1. *Risk Adjustment of Awards:* The amount of an incentive compensation award for an employee is adjusted based on measures that take into account the risk the employee's activities may pose to the organization. Such measures may be quantitative, or the size of a risk adjustment may be set judgmentally, subject to appropriate oversight.

2. *Deferral of Payment:* The actual payout of an award to an employee is delayed significantly beyond the end of the performance period, and the amounts paid are adjusted for actual losses or other aspects of performance that are realized or become better known only during the deferral period.[13] Deferred payouts may be altered according to risk outcomes either formulaically or judgmentally, subject to appropriate oversight. To be most effective, the deferral period should be sufficiently long to allow for the realization of a substantial portion of the risks from employee activities, and the measures of loss should be clearly explained to employees and closely tied to their activities during the relevant performance period.

3. *Longer Performance Periods:* The time period covered by the performance measures used in determining an employee's award is extended (for example, from one year to two or more years). Longer performance periods and deferral of payment are related in that both methods allow awards or payments to be made after some or all risk outcomes are realized or better known.

4. *Reduced Sensitivity to Short-Term Performance:* The banking organization reduces the rate at which awards increase as an employee achieves higher levels of the relevant performance measure(s). Rather than offsetting risk-taking incentives associated with the use of short-term performance measures, this method reduces the magnitude of such incentives. This method also can include improving the quality and reliability of performance measures in taking into account both short-term and long-term risks, for example improving the reliability and accuracy of estimates of revenues and long-term profits upon which performance measures depend.[14]

13. The deferral-of-payment method is sometimes referred to in the industry as a "clawback." The term "clawback" also may refer specifically to an arrangement under which an employee must return incentive compensation payments previously received by the employee (and not just deferred) if certain risk outcomes occur. Section 304 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7243), which applies to chief executive officers and chief financial officers of public banking organizations, is an example of this more specific type of "clawback" requirement.

14. Performance targets may have a material effect on risk-taking incentives. Such targets may offer employees greater rewards for increments of performance that are above the target or may provide that awards will be granted only if

These methods for achieving balance are not exclusive, and additional methods or variations may exist or be developed. Moreover, each method has its own advantages and disadvantages. For example, where reliable risk measures exist, risk adjustment of awards may be more effective than deferral of payment in reducing incentives for imprudent risk-taking. This is because risk adjustment potentially can take account of the full range and time horizon of risks, rather than just those risk outcomes that occur or become more evident during the deferral period. On the other hand, deferral of payment may be more effective than risk adjustment in mitigating incentives to take hard-to-measure risks (such as the risks of new activities or products, or certain risks such as reputational or operational risk that may be difficult to measure with respect to particular activities), especially if such risks are likely to be realized during the deferral period. Accordingly, in some cases two or more methods may be needed in combination for an incentive compensation arrangement to be balanced.

The greater the potential incentives an arrangement creates for an employee to increase the risks associated with the employee's activities, the stronger the effect should be of the methods applied to achieve balance. Thus, for example, risk adjustments used to counteract a materially unbalanced compensation arrangement should have a similarly material impact on the incentive compensation paid under the arrangement. Further, improvements in the quality and reliability of performance measures themselves, for example, improving the reliability and accuracy of estimates of revenues and profits upon which performance measures depend, can significantly improve the degree of balance in risk-taking incentives.

Where judgment plays a significant role in the design or operation of an incentive compensation arrangement, strong policies and procedures, internal controls, and ex post monitoring of incentive compensation payments relative to actual risk outcomes are particularly important to help ensure that the arrangements as implemented are balanced and do not encourage imprudent risk-taking. For example, if a banking organization relies to a significant degree on the judgment of one or more managers to ensure that the incentive compensation awards to employees are appropriately risk-adjusted, the organization should have policies and procedures that describe how managers are expected to exercise that judgment to achieve balance and that provide for the manager(s) to receive appropriate available information about the employee's risk-taking activities to make informed judgments.

Large complex banking organizations. Methods and practices for making compensation sensitive to risk are likely to evolve rapidly during the next few years, driven in part by the efforts of supervisors and other stakeholders. LCBOs should actively monitor developments in the field and should incorporate into their incentive compensation systems new or emerging methods or practices that are likely to improve the organization's long-term financial well-being and safety and soundness.

- *The manner in which a banking organization seeks to achieve balanced incentive compensation arrangements should be tailored to account for the differences between employees—including the substantial differences between senior executives and other employees—as well as between banking organizations.*

Activities and risks may vary significantly both across banking organizations and across employees within a particular banking organization. For example, activities, risks, and incentive compensation practices may differ materially among banking organizations based on, among other things, the scope or complexity of activities conducted and the business strategies pursued by the organizations. These differences mean that methods for achieving balanced compensation arrangements at one organization may not be effective in restraining incentives to engage in imprudent risk-taking at another organization. Each organization is responsible for ensuring that its incentive compensation arrangements are consistent with the safety and soundness of the organization.

Moreover, the risks associated with the activities of one group of non-executive employees (e.g., loan originators) within a banking organization may differ significantly from those of another group of non-executive employees (e.g., spot foreign exchange traders) within the organization. In addition, reliable quantitative mea-

a target is met or exceeded. Employees may be particularly motivated to take imprudent risk in order to reach performance targets that are aggressive but potentially achievable.

sures of risk and risk outcomes are unlikely to be available for a banking organization as a whole, particularly a large, complex organization. This factor can make it difficult for banking organizations to achieve balanced compensation arrangements for senior executives who have responsibility for managing risks on an organization-wide basis solely through use of the risk-adjustment-of-award method.

Furthermore, the payment of deferred incentive compensation in equity (such as restricted stock of the organization) or equity-based instruments (such as options to acquire the organization's stock) may be helpful in restraining the risk-taking incentives of senior executives and other covered employees whose activities may have a material effect on the overall financial performance of the organization. However, equity-related deferred compensation may not be as effective in restraining the incentives of lower-level covered employees (particularly at large organizations) to take risks because such employees are unlikely to believe that their actions will materially affect the organization's stock price.

Banking organizations should take account of these differences when constructing balanced compensation arrangements. For most banking organizations, the use of a single, formulaic approach to making employee incentive compensation arrangements appropriately risk-sensitive is likely to result in arrangements that are unbalanced at least with respect to some employees.[15]

Large complex banking organizations. Incentive compensation arrangements for senior executives at LCBOs are likely to be better balanced if they involve deferral of a substantial portion of the executives' incentive compensation over a multi-year period in a way that reduces the amount received in the event of poor performance, substantial use of multi-year performance periods, or both. Similarly, the compensation arrangements for senior executives at LCBOs are likely to be better balanced if a significant portion of the incentive compensation of these executives is paid in the form of equity-based instruments that vest over multiple years, with the number of instruments ultimately received dependent on the performance of the organization during the deferral period.

The portion of the incentive compensation of other covered employees that is deferred or paid in the form of equity-based instruments should appropriately take into account the level, nature, and duration of the risks that the employees' activities create for the organization and the extent to which those activities may materially affect the overall performance of the organization and its stock price. Deferral of a substantial portion of an employee's incentive compensation may not be workable for employees at lower pay scales because of their more limited financial resources. This may require increased reliance on other measures in the incentive compensation arrangements for these employees to achieve balance.

- *Banking organizations should carefully consider the potential for "golden parachutes" and the vesting arrangements for deferred compensation to affect the risk-taking behavior of employees while at the organizations.*

Arrangements that provide for an employee (typically a senior executive), upon departure from the organization or a change in control of the organization, to receive large additional payments or the accelerated payment of deferred amounts without regard to risk or risk outcomes can provide the employee significant incentives to expose the organization to undue risk. For example, an arrangement that provides an employee with a guaranteed payout upon departure from an organization, regardless of performance, may neutralize the effect of any balancing features included in the arrangement to help prevent imprudent risk-taking.

Banking organizations should carefully review any such existing or proposed arrangements (sometimes called "golden parachutes") and the potential impact of such arrangements on the organization's safety and soundness. In appropriate circumstances an organization should consider including balancing features—such as risk adjustment or deferral requirements that extend past the employee's departure—in the arrangements to mitigate the potential for the arrangements to encourage imprudent risk-taking. In all cases, a banking organization should ensure that the structure and terms of any golden parachute arrangement entered into by the organization do

15. For example, spreading payouts of incentive compensation awards over a standard three-year period may not appropriately reflect the differences in the type and time horizon of risk associated with the activities of different groups of employees, and may not be sufficient by itself to balance the compensation arrangements of employees who may expose the organization to substantial longer-term risks.

not encourage imprudent risk-taking in light of the other features of the employee's incentive compensation arrangements.

Large complex banking organizations. Provisions that require a departing employee to forfeit deferred incentive compensation payments may weaken the effectiveness of the deferral arrangement if the departing employee is able to negotiate a "golden handshake" arrangement with the new employer.[16] This weakening effect can be particularly significant for senior executives or other skilled employees at LCBOs whose services are in high demand within the market.

Golden handshake arrangements present special issues for LCBOs and supervisors. For example, while a banking organization could adjust its deferral arrangements so that departing employees will continue to receive any accrued deferred compensation after departure (subject to any clawback or malus[17]), these changes could (1) reduce the employee's incentive to remain at the organization and, thus, weaken an organization's ability to retain qualified talent, which is an important goal of compensation, and (2) create conflicts of interest. Moreover, actions of the hiring organization (which may or may not be a supervised banking organization) ultimately may defeat these or other risk-balancing aspects of a banking organization's deferral arrangements. LCBOs should monitor whether golden handshake arrangements are materially weakening the organization's efforts to constrain the risk-taking incentives of employees. The Federal Reserve will continue to work with banking organizations and others to develop appropriate methods for addressing any effect that such arrangements may have on the safety and soundness of banking organizations.

- *Banking organizations should effectively communicate to employees the ways in which incentive compensation awards and payments will be reduced as risks increase.*

In order for the risk-sensitive provisions of incentive compensation arrangements to affect employee risk-taking behavior, the organization's employees need to understand that the amount of incentive compensation that they may receive will vary based on the risk associated with their activities. Accordingly, banking organizations should ensure that employees covered by an incentive compensation arrangement are informed about the key ways in which risks are taken into account in determining the amount of incentive compensation paid. Where feasible, an organization's communications with employees should include examples of how incentive compensation payments may be adjusted to reflect projected or actual risk outcomes. An organization's communications should be tailored appropriately to reflect the sophistication of the relevant audience(s).

Principle 2: Compatibility with Effective Controls and Risk-Management

A banking organization's risk-management processes and internal controls should reinforce and support the development and maintenance of balanced incentive compensation arrangements.

In order to increase their own compensation, employees may seek to evade the processes established by a banking organization to achieve balanced compensation arrangements. Similarly, an employee covered by an incentive compensation arrangement may seek to influence, in ways designed to increase the employee's pay, the risk measures or other information or judgments that are used to make the employee's pay sensitive to risk.

Such actions may significantly weaken the effectiveness of an organization's incentive compensation arrangements in restricting imprudent risk-taking. These actions can have a particularly damaging effect on the safety and soundness of the organization if they result in the weakening of risk measures, information, or judgments that the organization uses for other risk-management, internal control, or financial purposes. In such cases, the employee's actions may weaken not only the balance of the orga-

16. Golden handshakes are arrangements that compensate an employee for some or all of the estimated, non-adjusted value of deferred incentive compensation that would have been forfeited upon departure from the employee's previous employment.

17. A malus arrangement permits the employer to prevent vesting of all or part of the amount of a deferred remuneration award. Malus provisions are invoked when risk outcomes are worse than expected or when the information upon which the award was based turns out to have been incorrect. Loss of unvested compensation due to the employee voluntarily leaving the firm is not an example of malus as the term is used in this guidance.

nization's incentive compensation arrangements, but also the risk-management, internal controls, and other functions that are supposed to act as a separate check on risk-taking. For this reason, traditional risk-management controls alone do not eliminate the need to identify employees who may expose the organization to material risk, nor do they obviate the need for the incentive compensation arrangements for these employees to be balanced. Rather, a banking organization's risk-management processes and internal controls should reinforce and support the development and maintenance of balanced incentive compensation arrangements.

- *Banking organizations should have appropriate controls to ensure that their processes for achieving balanced compensation arrangements are followed and to maintain the integrity of their risk-management and other functions.*

To help prevent damage from occurring, a banking organization should have strong controls governing its process for designing, implementing, and monitoring incentive compensation arrangements. Banking organizations should create and maintain sufficient documentation to permit an audit of the effectiveness of the organization's processes for establishing, modifying, and monitoring incentive compensation arrangements. Smaller banking organizations should incorporate reviews of these processes into their overall framework for compliance monitoring (including internal audit).

Large complex banking organizations. LCBOs should have and maintain policies and procedures that (1) identify and describe the role(s) of the personnel, business units, and control units authorized to be involved in the design, implementation, and monitoring of incentive compensation arrangements; (2) identify the source of significant risk-related inputs into these processes and establish appropriate controls governing the development and approval of these inputs to help ensure their integrity; and (3) identify the individual(s) and control unit(s) whose approval is necessary for the establishment of new incentive compensation arrangements or modification of existing arrangements.

An LCBO also should conduct regular internal reviews to ensure that its processes for achieving and maintaining balanced incentive compensation arrangements are consistently followed. Such reviews should be conducted by audit, compliance, or other personnel in a manner consistent with the organization's overall framework for compliance monitoring. An LCBO's internal audit department also should separately conduct regular audits of the organization's compliance with its established policies and controls relating to incentive compensation arrangements. The results should be reported to appropriate levels of management and, where appropriate, the organization's board of directors.

- *Appropriate personnel, including risk-management personnel, should have input into the organization's processes for designing incentive compensation arrangements and assessing their effectiveness in restraining imprudent risk-taking.*

Developing incentive compensation arrangements that provide balanced risk-taking incentives and monitoring arrangements to ensure they achieve balance over time requires an understanding of the risks (including compliance risks) and potential risk outcomes associated with the activities of the relevant employees. Accordingly, banking organizations should have policies and procedures that ensure that risk-management personnel have an appropriate role in the organization's processes for designing incentive compensation arrangements and for assessing their effectiveness in restraining imprudent risk-taking.[18] Ways that risk managers might assist in achieving balanced compensation arrangements include, but are not limited to

1. reviewing the types of risks associated with the activities of covered employees;
2. approving the risk measures used in risk adjustments and performance measures, as well as measures of risk outcomes used in deferred-payout arrangements; and
3. analyzing risk-taking and risk outcomes relative to incentive compensation payments.

Other functions within an organization, such as its control, human resources, or finance functions, also play an important role in helping

18. Involvement of risk-management personnel in the design and monitoring of these arrangements also should help ensure that the organization's risk-management functions can properly understand and address the full range of risks facing the organization.

ensure that incentive compensation arrangements are balanced. For example, these functions may contribute to the design and review of performance measures used in compensation arrangements or may supply data used as part of these measures.

- *Compensation for employees in risk-management and control functions should be sufficient to attract and retain qualified personnel and should avoid conflicts of interest.*

The risk-management and control personnel involved in the design, oversight, and operation of incentive compensation arrangements should have appropriate skills and experience needed to effectively fulfill their roles. These skills and experiences should be sufficient to equip the personnel to remain effective in the face of challenges by covered employees seeking to increase their incentive compensation in ways that are inconsistent with sound risk-management or internal controls. The compensation arrangements for employees in risk-management and control functions thus should be sufficient to attract and retain qualified personnel with experience and expertise in these fields that is appropriate in light of the size, activities, and complexity of the organization.

In addition, to help preserve the independence of their perspectives, the incentive compensation received by risk-management and control personnel staff should not be based substantially on the financial performance of the business units that they review. Rather, the performance measures used in the incentive compensation arrangements for these personnel should be based primarily on the achievement of the objectives of their functions (e.g., adherence to internal controls).

- *Banking organizations should monitor the performance of their incentive compensation arrangements and should revise the arrangements as needed if payments do not appropriately reflect risk.*

Banking organizations should monitor incentive compensation awards and payments, risks taken, and actual risk outcomes to determine whether incentive compensation payments to employees are reduced to reflect adverse risk outcomes or high levels of risk taken. Results should be reported to appropriate levels of management, including the board of directors where warranted and consistent with Principle 3 below. The monitoring methods and processes used by a banking organization should be commensurate with the size and complexity of the organization, as well as its use of incentive compensation. Thus, for example, a small, noncomplex organization that uses incentive compensation only to a limited extent may find that it can appropriately monitor its arrangements through normal management processes.

A banking organization should take the results of such monitoring into account in establishing or modifying incentive compensation arrangements and in overseeing associated controls. If, over time, incentive compensation paid by a banking organization does not appropriately reflect risk outcomes, the organization should review and revise its incentive compensation arrangements and related controls to ensure that the arrangements, as designed and implemented, are balanced and do not provide employees incentives to take imprudent risks.

Principle 3: Strong Corporate Governance

Banking organizations should have strong and effective corporate governance to help ensure sound compensation practices, including active and effective oversight by the board of directors.

Given the key role of senior executives in managing the overall risk-taking activities of an organization, the board of directors of a banking organization should directly approve the incentive compensation arrangements for senior executives.[19] The board also should approve and document any material exceptions or adjustments to the incentive compensation arrangements established for senior executives and should carefully consider and monitor the effects

19. As used in this guidance, the term ''board of directors'' is used to refer to the members of the board of directors who have primary responsibility for overseeing the incentive compensation system. Depending on the manner in which the board is organized, the term may refer to the entire board of directors, a compensation committee of the board, or another committee of the board that has primary responsibility for overseeing the incentive compensation system. In the case of FBOs, the term refers to the relevant oversight body for the firm's U.S. operations, consistent with the FBO's overall corporate and management structure.

of any approved exceptions or adjustments on the balance of the arrangement, the risk-taking incentives of the senior executive, and the safety and soundness of the organization.

The board of directors of an organization also is ultimately responsible for ensuring that the organization's incentive compensation arrangements for all covered employees are appropriately balanced and do not jeopardize the safety and soundness of the organization. The involvement of the board of directors in oversight of the organization's overall incentive compensation program should be scaled appropriately to the scope and prevalence of the organization's incentive compensation arrangements.

Large complex banking organizations and organizations that are significant users of incentive compensation. The board of directors of an LCBO or other banking organization that uses incentive compensation to a significant extent should actively oversee the development and operation of the organization's incentive compensation policies, systems, and related control processes. The board of directors of such an organization should review and approve the overall goals and purposes of the organization's incentive compensation system. In addition, the board should provide clear direction to management to ensure that the goals and policies it establishes are carried out in a manner that achieves balance and is consistent with safety and soundness.

The board of directors of such an organization also should ensure that steps are taken so that the incentive compensation system—including performance measures and targets—is designed and operated in a manner that will achieve balance.

- *The board of directors should monitor the performance, and regularly review the design and function, of incentive compensation arrangements.*

To allow for informed reviews, the board should receive data and analysis from management or other sources that are sufficient to allow the board to assess whether the overall design and performance of the organization's incentive compensation arrangements are consistent with the organization's safety and soundness. These reviews and reports should be appropriately scoped to reflect the size and complexity of the banking organization's activities and the prevalence and scope of its incentive compensation arrangements.

The board of directors of a banking organization should closely monitor incentive compensation payments to senior executives and the sensitivity of those payments to risk outcomes. In addition, if the compensation arrangement for a senior executive includes a clawback provision, then the review should include sufficient information to determine if the provision has been triggered and executed as planned.

The board of directors of a banking organization should seek to stay abreast of significant emerging changes in compensation plan mechanisms and incentives in the marketplace as well as developments in academic research and regulatory advice regarding incentive compensation policies. However, the board should recognize that organizations, activities, and practices within the industry are not identical. Incentive compensation arrangements at one organization may not be suitable for use at another organization because of differences in the risks, controls, structure, and management among organizations. The board of directors of each organization is responsible for ensuring that the incentive compensation arrangements for its organization do not encourage employees to take risks that are beyond the organization's ability to manage effectively, regardless of the practices employed by other organizations.

Large complex banking organizations and organizations that are significant users of incentive compensation. The board of an LCBO or other organization that uses incentive compensation to a significant extent should receive and review, on an annual or more frequent basis, an assessment by management, with appropriate input from risk-management personnel, of the effectiveness of the design and operation of the organization's incentive compensation system in providing risk-taking incentives that are consistent with the organization's safety and soundness. These reports should include an evaluation of whether or how incentive compensation practices may increase the potential for imprudent risk-taking.

The board of such an organization also should receive periodic reports that review incentive compensation awards and payments relative to risk outcomes on a backward-looking basis to determine whether the organization's incentive compensation arrangements may be promoting imprudent risk-taking. Boards of directors of

these organizations also should consider periodically obtaining and reviewing simulation analysis of compensation on a forward-looking basis based on a range of performance levels, risk outcomes, and the amount of risks taken.

- *The organization, composition, and resources of the board of directors should permit effective oversight of incentive compensation.*

The board of directors of a banking organization should have, or have access to, a level of expertise and experience in risk-management and compensation practices in the financial services industry that is appropriate for the nature, scope, and complexity of the organization's activities. This level of expertise may be present collectively among the members of the board, may come from formal training or from experience in addressing these issues, including as a director, or may be obtained through advice received from outside counsel, consultants, or other experts with expertise in incentive compensation and risk-management. The board of directors of an organization with less complex and extensive incentive compensation arrangements may not find it necessary or appropriate to require special board expertise or to retain and use outside experts in this area.

In selecting and using outside parties, the board of directors should give due attention to potential conflicts of interest arising from other dealings of the parties with the organization or for other reasons. The board also should exercise caution to avoid allowing outside parties to obtain undue levels of influence. While the retention and use of outside parties may be helpful, the board retains ultimate responsibility for ensuring that the organization's incentive compensation arrangements are consistent with safety and soundness.

Large complex banking organizations and organizations that are significant users of incentive compensation. If a separate compensation committee is not already in place or required by other authorities,[20] the board of directors of an LCBO or other banking organization that uses incentive compensation to a significant extent should consider establishing such a committee—reporting to the full board—that has primary responsibility for overseeing the organization's incentive compensation systems. A compensation committee should be composed solely or predominantly of non-executive directors. If the board does not have such a compensation committee, the board should take other steps to ensure that non-executive directors of the board are actively involved in the oversight of incentive compensation systems. The compensation committee should work closely with any board-level risk and audit committees where the substance of their actions overlap.

- *A banking organization's disclosure practices should support safe and sound incentive compensation arrangements.*

If a banking organization's incentive compensation arrangements provide employees incentives to take risks that are beyond the tolerance of the organization's shareholders, these risks are likely to also present a risk to the safety and soundness of the organization.[21] To help promote safety and soundness, a banking organization should provide an appropriate amount of information concerning its incentive compensation arrangements for executive and non-executive employees and related risk-management, control, and governance processes to shareholders to allow them to monitor and, where appropriate, take actions to restrain the potential for such arrangements and processes that encourage employees to take imprudent risks. Such disclosures should include information relevant to employees other than senior executives. The scope and level of the information disclosed by the organization should be tailored to the nature and complexity of the organization and its incentive compensation arrangements.[22]

- *Large complex banking organizations should follow a systematic approach to developing a compensation system that has balanced incentive compensation arrangements.*

20. See New York Stock Exchange Listed Company Manual Section 303A.05(a); Nasdaq Listing Rule 5605(d); Internal Revenue Code section 162(m) (26 U.S.C. 162(m)).

21. On the other hand, as noted previously, compensation arrangements that are in the interests of the shareholders of a banking organization are not necessarily consistent with safety and soundness.

22. A banking organization also should comply with the incentive compensation disclosure requirements of the federal securities law and other laws as applicable. See, for example, Proxy Disclosure Enhancements, SEC Release Nos. 33-9089, 34-61175, 74 F.R. 68334 (Dec. 23, 2009) (to be codified at 17 C.F.R. 229 and 249).

At banking organizations with large numbers of risk-taking employees engaged in diverse activities, an ad hoc approach to developing balanced arrangements is unlikely to be reliable. Thus, an LCBO should use a systematic approach—supported by robust and formalized policies, procedures, and systems—to ensure that those arrangements are appropriately balanced and consistent with safety and soundness. Such an approach should provide for the organization effectively to:

1. Identify employees who are eligible to receive incentive compensation and whose activities may expose the organization to material risks. These employees should include
   a. senior executives and others who are responsible for oversight of the organization's firm-wide activities or material business lines;
   b. individual employees, including non-executive employees, whose activities may expose the organization to material amounts of risk; and
   c. groups of employees who are subject to the same or similar incentive compensation arrangements and who, in the aggregate, may expose the organization to material amounts of risk;
2. Identify the types and time horizons of risks to the organization from the activities of these employees;
3. Assess the potential for the performance measures included in the incentive compensation arrangements for these employees, those that encourage employees to take imprudent risks;
4. Include balancing elements (such as risk adjustments or deferral periods) within the incentive compensation arrangements for these employees, that are reasonably designed to ensure that the arrangement will be balanced in light of the size, type, and time horizon of the inherent risks of the employees' activities;
5. Communicate to the employees the ways in which their incentive compensation awards or payments will be adjusted to reflect the risks of their activities to the organization; and
6. Monitor incentive compensation awards, payments, risks taken, and risk outcomes for these employees and modify the relevant arrangements if payments made are not appropriately sensitive to risk and risk outcomes.

CONCLUSION ON SOUND INCENTIVE COMPENSATION

Banking organizations are responsible for ensuring that their incentive compensation arrangements do not encourage imprudent risk-taking behavior and are consistent with the safety and soundness of the organization. The Federal Reserve expects banking organizations to take prompt action to address deficiencies in their incentive compensation arrangements or related risk-management, control, and governance processes.

The Federal Reserve intends to actively monitor the actions taken by banking organizations in this area and will promote further advances in designing and implementing balanced incentive compensation arrangements. Where appropriate, the Federal Reserve will take supervisory or enforcement action to ensure that material deficiencies that pose a threat to the safety and soundness of the organization are promptly addressed. The Federal Reserve also will update this guidance as appropriate to incorporate best practices as they develop over time.

INTRODUCTION

From a regulator's standpoint, the essential purpose of bank earnings, both current and accumulated, is to absorb losses and augment capital. Earnings is the initial safeguard against the risks that a bank incurs in the course of doing business, and represents a bank's first line of defense against capital depletion resulting from a decline in the value of its assets. This section is designed to provide a high-level overview for examiners in assessing a bank's earning through the use of analytical review techniques. Examiners need to remain cognizant of the inextricable links among capital, asset quality, earnings, liquidity, and market risk sensitivity.

GENERAL EXAMINATION APPROACH

As part of the off-site preparation for an on-site examination, examiners review and analyze a bank's financial condition. (See the manual sections entitled, "Examination Strategy and Risk-Focused Examinations" and "Federal Reserve System Bank Surveillance Program.") This analysis is meant to identify potential problem areas and to develop the examination scope so that proper staff levels and appropriate examination procedures can be used.

The analysis of earnings includes all bank operations and activities. When evaluating earnings, examiners should develop an understanding of the bank's core business activities. Core activities are those operations that are part of a bank's normal or continuing business. Examiners should understand a bank's composition of earnings and sustainability of the various earnings components. This would include balance-sheet composition, particularly the volume and type of earning assets and off-balance-sheet items, if applicable.

ANALYTICAL REVIEW

In performing the analytical review of a bank, examiners should use the most recent Uniform Bank Performance Report (UBPR) as well as the most recent financial statements and other related financial information that supports the source and trend in the bank's earnings. A well-performed analytical review provides examiners with an understanding of the bank's operations. An analytical review of bank earnings highlights matters of interest and potential problem situations which, examiners will need to address with the bank. In reviewing and assessing a bank's earning, examiners perform level and trend analysis of financial report data and ratios as well as reviewing other metrics. Analytical review is based on the assumption that period-to-period balances and ratios are free from significant error considering the procedures relating to income and expenses, and regulatory reports conducted by internal or external auditors. (See the manual section entitled, "Internal Control and Audit Function, Oversight, and Outsourcing," for a discussion of factors to consider in reviewing the audit work of others.)

Analytical Tools

The UBPR and the bank's financial statements are key sources of analysis for examination staff. Bank-prepared statements and supplemental schedules, if available, facilitate an in-depth analytical review. The information from those schedules may give examiners considerable insight into the interpretation of the bank's basic financial statements. To properly understand and interpret a particular bank's financial and statistical data, examiners should be familiar with current economic and industry conditions, including any idiosyncratic cyclical or seasonal factors in the nation, region, and local area that may have an affect on the bank's earnings. Economic and industry information, reports, and journals are useful informational sources of industry conditions and trends. Finally, examiners should be knowledgeable about new banking laws and new accounting standards or methodologies that could have a material effect on financial institutions' business and earnings.

UBPR

The information used to prepare UBPRs are largely based on the Consolidated Reports of

Condition and Income (Call Report). Each UBPR also contains corresponding average data for the bank's peer group (a group of banks of similar asset size and reporting characteristics) and percentile rankings for most ratios. The UBPR facilitates the evaluation of a bank's current condition, trends in its financial performance, and comparisons with the performance of its peer group.

The user's guide for the UBPR explains how a structured approach to financial analysis should be followed.[1] This approach breaks down a bank's income stream into its major components of interest margin performance, overhead, noninterest income, loan-loss provisions, tax factors, and extraordinary items. These major components can then be broken down into various subcomponents. Also, examiners should analyze the balance-sheet composition along with economic conditions to understand the source and future variability of a bank's income stream.

The dollar amounts displayed for most income and expense items in the UBPR are shown for the year-to-date period. However, to allow comparison of ratios between quarters, income and expense and related data used in certain ratios are annualized for interim reporting periods. Thus, the income or expense item is multiplied by the indicated factor listed below before dividing it by the corresponding asset or liability. The UBPR annualization factors are

- March 4.0,
- June 2.0, and
- September 1.3333.

Income and expense information reported on the December 31 Call Report is not annualized. Since the year-end UBPR represents a full fiscal year.

Frequently, examiners need a more detailed and current review of a bank's financial condition than that provided by the UBPR. Under certain circumstances, UBPR procedures may need to be supplemented because—

- asset-quality information must be linked to the income stream;
- more detailed information is necessary on asset-liability maturities and matching;
- more detailed information is necessary on other liquidity aspects, as they may affect earnings;
- yield or cost information, which may be difficult to interpret from the report, is needed;
- certain income or expense items may need clarification, as well as normal examination validation;
- volume information, such as the number of demand deposits, certificates of deposit, and other accounts, is not reported, and vulnerability in a bank subject to concentrations normally should be considered;
- components of interest and fees on loans are not reported separately by category of loan; thus, adverse trends in the loan portfolio may not be detected (for example, the yield of a particular bank's loan portfolio may be similar to those of its peer group, but examiners may detect an upward trend in yields for a specific category of loans. That upward trend might be partially or wholly offset by a downward trend of yields in another category of loans, and examiners should consider further investigating the circumstances applicable to each of those loan categories. A change in yields could be a result of a change in the bank's business model or risk "appetite" for certain types of loans or may indicate a change in loan underwriting standards.); or
- income or expense resulting from a change in the bank's operations, such as the opening of a new branch or starting of a mortgage banking activity or trust department, may skew performance ratios. (When there has been a significant change in a bank's operations, examiners should analyze the potential impact of the change on future bank earnings.)

Review of Management's Budget and Financial Statements

In addition to UBPR analysis, examiners should incorporate a review of management's budget and/or financial projections. In reviewing a bank's projections and individual variances from its operating budget, examiners should be able to identify the sources and trends in the bank's prior and future earnings. Examiners should also verify the reasonableness of the budgeted amounts, frequency of budget review by bank management and the board of directors, and level of involvement of key bank personnel in the budget process.

In reviewing a bank's financial statements,

1. The Federal Financial Institutions Examination Council (FFIEC) provides additional information on the UBPR, including the UBPR User's Guide at www.ffiec.gov/ubpr.htm.

examiners should be cognizant of new accounting standards or changes in accounting methodologies. In addition, alternative accounting treatments for similar transactions among peer banks also should be considered because they may produce significantly different results. The analytical review must be based on figures derived under valid accounting practices consistently applied, particularly in the accrual areas. Accordingly, during the analytical review, examiners should work with Reserve Bank accounting specialists to determine any material inconsistencies in the application of accounting principles.

Review of Nonrecurring and Extraordinary Items

When assessing earnings, examiners should be aware of nonrecurring events or actions that have affected a bank's earnings performance, positively or negatively, and should adjust earnings on a tax equivalent (TE) basis for comparison purposes. Although the analysis should reflect adjustments for non-recurring events, examiners should also include within their analysis the impact that these items had on overall earnings performance. Examples of events that may affect earnings include adoption of new accounting standards, extraordinary items, or other actions taken by management that are not considered part of a bank's normal operations such as sales of securities for tax purposes or for some other reason unrelated to active management of the securities portfolio.

The exclusion of nonrecurring events from the analysis allows examiners to analyze the profitability of a bank's core operations without the distortions caused by non-recurring items. By adjusting for these distortions, examiners are better able to compare a bank's current earnings performance against the bank's past performance and industry norms (for example, peer group data).

Compliance with Laws and Regulations Relating to Earnings and Dividends

Examiners should consider the interrelationships that exist among the dividend-payout ratio, the rate of growth of retained earnings, and the bank's ability to cover losses and maintain adequate capital. A bank's earnings should also be more than sufficiently adequate in relation to its current dividend rate. In particular, examiners should consider whether a bank's dividend rate is prudent relative to its financial position and not based on overly optimistic earnings scenarios. See SR-09-4, "Applying Supervisory Guidance and Regulations on the Payment of Dividends, Stock Redemptions, and Stock Repurchases at Bank Holding Companies."[2] Prudent management dictates that a bank should consider the curtailment of the dividend rate if capital is inadequate and greater earnings retention is required. If it appears that a bank's dividend payout isexcessive or that there is a record of recent operating losses, examiners should refer to sections 5199(b) and 5204 of the United States Revised Statutes and section 208.19 of Regulation H which restrict state member bank dividends. See also this manual's section entitled, "Dividends."

ASSIGNING THE EARNINGS RATING

After performing the appropriate examination procedures and documenting the supervisory assessment of a bank, examiners assign a component Uniform Financial Institution Ratings System rating based on an evaluation of a banks earnings. Examiners assign a rating that addresses the quantity and trend of a bank's earnings, as well as factors that may affect the sustainability or quality of earnings. The quantity as well as the quality of a bank's earnings can be affected by excessive or inadequately managed credit risk that may result in loan losses and require additions to the allowance for loan and lease losses, or by high levels of market risk that may unduly expose an institution's earnings to volatility in interest rates.[3] The quality of earnings may also be diminished by undue reliance on extraordinary gains, nonrecurring events, or favorable tax effects. Future earnings may be adversely affected by an inability to forecast or control funding and operating

2. See also the *Bank Holding Company Supervision Manual* for a discussion of the Board's "Policy Statement on the Payment of Cash Dividends by State Member Banks and Bank Holding Companies."

3. See this manual's section entitled, "Allowance for Loan and Lease Losses," for more information.

expenses, improperly executed or ill-advised business strategies, or poorly managed or uncontrolled exposure to other risks.

Examiners base their rating of a bank's earnings based upon, but not limited to, an assessment of the following evaluation factors:

- the level of earnings, including trends and stability
- the bank's ability to provide for adequate capital through retained earnings
- the quality and sources of earnings
- the level of expenses in relation to the bank's operations
- the adequacy of the bank's budgeting systems, forecasting processes, and management information systems in general
- the adequacy of the bank's provisions for the allowance for loan and lease losses and other valuation allowance accounts
- the earnings exposure to market risk such as interest rate, foreign exchange, and price risks

1. To determine whether profit planning and budgeting practices are adequate.
2. To determine whether internal controls are adequate.
3. To assess whether the audit or independent review functions adequate.
4. To determine whether information and communication systems are adequate and accurate.
5. To determine whether earnings are sufficient to support operations, provide for funding of the allowance for loan and lease losses and augment capital.
6. To assess whether earnings are sustainable.
7. To determine whether board and senior management effectively supervise this area.

1. Review previous reports of examination, prior examination work papers, and file correspondence for an overview of any previously identified earnings concerns, strengths, or other considerations.
2. Review recent audits and independent reviews to identify deficiencies concerning the reliability of management information systems (MIS) that may affect the quality and reliability of reported earnings.
3. Review management's remedial actions to correct examination and audit deficiencies.
4. Discuss with management any recent or planned changes in strategic objectives and their implications for profit plans.
5. Review board and committee minutes and management reports to determine the adequacy/quality of MIS systems and reports.
6. Review recent Uniform Bank Performance Reports (UBPR) to develop an initial assessment of overall earnings performance. Consider the impact of Chapter S tax filing status when selecting performance ratios to review.
7. Compare financial statements, UBPRs, and Consolidated Reports of Condition and Income (Call Reports) to determine if there have been any significant changes that could materially affect earnings performance.

PROFIT PLANNING AND BUDGETING PRACTICES

8. Review strategic plans, profit plans, and budgets to determine if the underlying assumptions are realistic. Determine the sources of input for profit plans and budgets. Profit plans and budgets should consider the following areas with detail appropriate for the size, complexity, and risk profile of the bank:
   - anticipated funding of the allowance for loan and lease losses
   - anticipated level and volatility of interest rates
   - interest rate and maturity mismatches
   - local and national economic conditions
   - funding strategies
   - new products and business lines
   - asset and liability mix and pricing
   - growth objectives
   - capital requirements
9. Assess the timeliness of preparing and approving the profit plans and budgets.
10. Compare earnings performance to budget forecasts. Determine whether management compares budgeted performance to actual performance on a periodic basis, modifies projections when interim circumstances change significantly, and evaluates budget forecasts under multiple stress scenarios.

INTERNAL CONTROLS

11. Review management's procedures to prevent, detect, and correct errors with respect to MIS.
12. Determine whether the income and expense posting, reconcilement, and review functions are independent of each other. Consider testing selected income, expense, and balance sheet items to observe the operational flow of transactions and to assess the potential for fraud from internal control weaknesses. Areas commonly selected for review are
    - large volumes of other income (miscellaneous, service fees, or any other unusual accounts);
    - proper amortization of loan origination fees;
    - insider expense accounts;
    - management fees or other payments to affiliates;
    - significant legal fees;
    - prepaid accounts;
    - stale items; and
    - expenses accrued and unpaid.
13. Determine whether significant or nonrecurring income, expenses, and capital charges are reviewed and appropriately authorized.

14. Determine whether insider or affiliate-related income and expense items are routinely reviewed for authorization, appropriateness, and compliance with laws and regulations.

AUDIT OR INDEPENDENT REVIEW

15. Determine whether the audit or independent review program provides sufficient coverage of earnings activities relative to the bank's size, complexity, and risk profile. Consider the following:
    - adherence with profit planning objectives, accounting standards, and Consolidated Report of Income Instructions
    - transaction testing completed to assure income and expenses are accurately recorded
    - separation of duties and internal controls
    - adequacy, accuracy, and timeliness of reports to senior management and the board
    - recommended corrective action when warranted
    - verification of implementation and effectiveness of corrective action

INFORMATION AND COMMUNICATION SYSTEMS

16. Determine whether managerial reports provide sufficient information relative to the size and risk profile of the institution.
17. Evaluate the accuracy and timeliness of reports produced for the board and senior management. Reports may include
    - periodic earnings results;
    - budget variance analyses;
    - income and expense projections;
    - non-recurring or cyclical items;
    - exposure to interest rate/market risk;
    - large item reviews;
    - insider related transaction disclosures; and
    - tax planning analyses.
18. Validate the accuracy of Call Reports as appropriate. Use bank work papers, the general ledger, downloaded exception reports, and interviews with bank personnel to verify the accuracy of the appropriate Call Report schedules.

RATIO AND TREND ANALYSIS

20. Assess the level, trend, and sustainability of the return on average assets relative to historical performance, peer comparisons, the organization's risk profile, balance sheet structure/composition, and local and national economic conditions. Consideration should also be given to the amount and volatility of income from high-risk assets, asset concentrations, non-recurring items, and accounting practices subject to management discretion (which could manipulate earnings). Identify and assess any areas needing further investigation.
21. Evaluate the level, trend, and stability of the bank's net interest margin. Discuss with examiners reviewing credit, market, and liquidity risks the impact to present and future earnings performance from potential changes in asset quality, market fluctuations, and interest rates.
22. Evaluate the level and trend of overhead expenses. Consider the impact of present and future strategic initiatives (for example, branch openings/closings, increases/decreases in operating staff or executive officers).
23. Evaluate the level, trend, and sources of non-interest income. Discuss with management any projections for changes in fee structures. Consider the impact of changes in interest rates and market conditions on mortgage banking income, securities gains, or other non-interest revenue sources.
24. Review the level and trend of provisions for loan and lease losses and the relationship to actual loan losses to determine the impact of asset quality on earnings. Discuss with the examiner(s) responsible for loan review the potential need for additional provision expenses resulting from examination findings.
25. Review the level, trend, and expected frequency of non-operating gains and losses and their impact on earnings.
26. Consider the impact to earnings from purchased-impaired accounting practices,

and if applicable, discuss with an accounting specialist.

27. Determine whether there have been or are expected to be any nonrecurring events and consider their impact to earnings performance. If necessary for comparison purposes, evaluate this impact on a tax-equivalent basis.
28. Evaluate the level and trend of income tax payments recognizing the institution's basis for filing taxes (for example, Subchapter S, tax allocation agreement).
29. Assess the ability of earnings to support capital growth under current, projected, and stressed conditions. Review the earnings retention rate in comparison to past and forecasted growth rates.
30. Evaluate the earnings impact of activities with affiliated organizations.

BOARD AND SENIOR MANAGEMENT SUPERVISION

31. Determine whether the board and senior management review bank earnings and appropriately responds to significant budget deviations.
32. Assess compliance with bank policies, applicable regulations, and governing accounting standards. If applicable, determine compliance with outstanding formal or informal enforcement actions.

Analytical Review and Income and Expense

Internal Control Questionnaire

Effective date March 1984

Section 4010.4

Review the bank's internal controls, policies, practices and procedures over income and expenses. The bank's system should be documented in a complete and concise manner and should include, where appropriate, narrative descriptions, flowcharts, copies of forms used and other pertinent information. Items marked with an asterisk require substantiation by observation or testing.

GENERAL

1. Does the bank have a budget? If so:
   a. Is it reviewed and approved by managerial personnel and/or the board of directors?
   b. Is it periodically reviewed and updated for changed conditions?
   c. Are periodic statements compared to budget and are explanations of variances reviewed by managment?
   d. Is a separate budget prepared by the manager of each department or division?
2. Does the bank's accounting system provide sufficiently detailed breakdowns of accounts to enable it to analyze fluctuations?

*3. Are the general books of the bank maintained by someone who does not have access to cash?

4. Are all general ledger entries processed through the proof department?
5. Are all entries to the general ledger supported by a general ledger ticket?
6. Do general ledger tickets, both debit and credit, bear complete approvals, descriptions and an indication of the offset?

*7. Are all general ledger entries approved by a responsible person other than the general ledger bookkeeper or person associated with its preparation?

8. Is the general ledger posted daily?
9. Is a daily statement of condition prepared?

*10. Are corrections to ledgers made by posting a correcting entry and not by erasing (manual system) or deleting (computerized system) the incorrect entry?

11. Are supporting worksheets or other records maintained on accrued expenses and taxes?
12. Are those supporting records periodically reconciled with the appropriate general ledger controls?

PURCHASES

*13. If the bank has a separate purchasing department, is it independent of the accounting and receiving departments?

*14. Are purchases made only on the basis of requisitions signed by authorized individuals?

*15. Are all purchases routed through a purchasing department or personnel functioning in that capacity?

16. Are all purchases made by means of prenumbered purchase orders sent to vendors?
17. Are all invoices received checked against purchase orders and receiving reports?
18. Are all invoices tested for clerical accuracy?
19. Are invoice amounts credited to their respective accounts and tested periodically for accuracy?

DISBURSEMENTS

*20. Is the payment for all purchases, except minor items, made by official checks?

*21. Does the official signing the check review all supporting documents?

*22. Are supporting vouchers and invoices cancelled to prevent re-use?

*23. Are duties and responsibilities in the following areas segregated?
   a. Authorization to issue expense checks?
   b. Preparation of expense checks?
   c. Signing of expense checks?
   d. Sending of expense checks?
   e. Use and storage of facsimile signatures?
   f. General ledger posting?
   g. Subsidiary ledger posting?

PAYROLL

24. Is the payroll department separate from the personnel department?
25. Are signed authorizations on file for all payroll deductions including W-4s for withholding?
26. Are salaries authorized by the board of directors or its designated committee?

27. Are individual wage rates authorized in writing by an authorized officer?
28. Are vacation and sick leave payments fixed or authorized?
29. Are payrolls paid from a special bank account or directly credited to the employee's demand deposit account?
30. Are time records reviewed and signed by the employee's supervisor?
31. Are double checks made of hours, rates, deductions, extension, and footings?
32. Are payroll signers independent of the persons approving hours worked and preparation of the payroll?
33. If a check signing machine is used, are controls over its use adequate (such as a dual control)?
34. Are payrolls subject to final officer approval?
35. Are the names of persons leaving employment of the bank reported promptly, in writing, to the payroll department?
36. Are payroll expense distributions reconciled with the general payroll payment records?

CONCLUSION

37. Is the foregoing information an adequate basis for evaluating internal control in that there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
38. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate, inadequate).

WHAT'S NEW IN THIS REVISED SECTION

This section is being revised to include the March 1, 2016, "Interagency Guidance on Funds Transfer Pricing Related to Funding Contingency Risks." The guidance (refer to appendix 3 of this section) was issued to address weaknesses observed in large financial institutions' funds transfer pricing (FTP) practices related to funding risk (including interest rate and liquidity components) and contingent liquidity risk. The interagency guidance builds on the principles of sound liquidity risk management. FTP is an important tool for managing a firm's balance sheet structure and measuring risk-adjusted profitability. By allocating funding and contingent liquidity risks to business lines, products, and activities within a firm, FTP influences the volume and terms of new business and ongoing portfolio composition. If done effectively, FTP promotes more resilient, sustainable business models. (Refer to SR-16-3.)

FACTORS INFLUENCING LIQUIDITY MANAGEMENT AND TYPES OF LIQUIDITY RISK

Liquidity is a financial institution's capacity to meet its cash and collateral obligations without incurring unacceptable losses. Adequate liquidity is dependent upon the institution's ability to efficiently meet both expected and unexpected cash flows and collateral needs without adversely affecting either daily operations or the financial condition of the institution. An institution's obligations and the funding sources used to meet them depend significantly on its business mix, balance-sheet structure, and the cash-flow profiles of its on- and off-balance-sheet obligations. In managing their cash flows, institutions confront various situations that can give rise to increased liquidity risk. These include funding mismatches, market constraints on the ability to convert assets into cash or in accessing sources of funds (i.e., market liquidity), and contingent liquidity events. Changes in economic conditions or exposure to credit, market, operation, legal, and reputation risks also can affect an institution's liquidity-risk profile and should be considered in the assessment of liquidity and asset/liability management.

Liquidity risk is the risk to an institution's financial condition or safety and soundness arising from its inability (whether real or perceived) to meet its contractual obligations. Because banking organizations employ a significant amount of leverage in their business activities—and need to meet contractual obligations in order to maintain the confidence of customers and fund providers—adequate liquidity is critical to an institution's ongoing operation, profitability, and safety and soundness.

To ensure it has adequate liquidity, an institution must balance the costs and benefits of liquidity: Too little liquidity can expose an institution to an array of significant negative repercussions arising from its inability to meet contractual obligations. Conversely, too much liquidity can entail substantial opportunity costs and have a negative impact on the firm's profitability.

Effective liquidity management entails the following three elements:

- assessing, on an ongoing basis, the current and expected future needs for funds, and ensuring that sufficient funds or access to funds exists to meet those needs at the appropriate time
- providing for an adequate cushion of liquidity with a stock of liquid assets to meet unanticipated cash-flow needs that may arise from a continuum of potential adverse circumstances that can range from high-probability/low-severity events that occur in daily operations to low-probability/high-severity events that occur less frequently but could significantly affect an institution's safety and soundness
- striking an appropriate balance between the benefits of providing for adequate liquidity to mitigate potential adverse events and the cost of that liquidity

The primary role of liquidity-risk management is to (1) prospectively assess the need for funds to meet obligations and (2) ensure the availability of cash or collateral to fulfill those needs at the appropriate time by coordinating the various sources of funds available to the

Note: The guidance complements existing guidance in the *Bank Holding Company Supervision Manual* (section 4010.2) and various SR-letters (see the "References" section).

institution under normal and stressed conditions. Funds needs arise from the myriad of banking activities and financial transactions that create contractual obligations to deliver funds, including business initiatives for asset growth, the provision of various financial products and transaction services, and expected and unexpected changes in assets and the liabilities used to fund assets. Liquidity managers have an array of alternative sources of funds to meet their liquidity needs. These sources generally fall within one of four broad categories:

- net operating cash flows
- the liquidation of assets
- the generation of liabilities
- an increase in capital funds

Funds obtained from operating cash flows arise from net interest payments on assets; net principal payments related to the amortization and maturity of assets; and the receipt of funds from various types of liabilities, transactions, and service fees. Institutions obtain liquidity from operating cash flows by managing the timing and maturity of their asset and liability cash flows, including their ongoing borrowing and debt-issuance programs.

Funds can also be obtained by reducing or liquidating assets. Most institutions incorporate scheduled asset maturities and liquidations as part of their ongoing management of operating cash flows. They also use the potential liquidation of a portion of their assets (generally a portion of the investment portfolio) as a contingent source of funds to meet cash needs under adverse liquidity circumstances. Such contingent funds need to be unencumbered for the purposes of selling or lending the assets and are often termed *liquidity reserves* or *liquidity warehouses* and are a critical element of safe and sound liquidity management. Assessments of the value of unencumbered assets should represent the amount of cash that can be obtained from monetized assets under normal as well as stressed conditions.

Asset securitization is another method that some institutions use to fund assets. Securitization involves the transformation of on-balance-sheet loans (e.g., auto, credit card, commercial, student, home equity, and mortgage loans) into packaged groups of loans in various forms, which are subsequently sold to investors. Depending on the business model employed, securitization proceeds can be both a material source of ongoing funding and a significant tool for meeting future funding needs. Securitization markets may provide a good source of funding; however, institutions should be cautious in relying too heavily on this market as it has been known to shutdown under market stress situations.

Funds are also generated through deposit-taking activities, borrowings, and overall liability management. Borrowed funds may include secured lending and unsecured debt obligations across the maturity spectrum. In the short term, borrowed funds may include purchased fed funds and securities sold under agreements to repurchase (repos). Longer-term borrowed funds may include various types of deposit products, collateralized loans, and the issuance of corporate debt. Depending on their contractual characteristics and the behavior of fund providers, borrowed funds can vary in maturity and availability because of their sensitivity to general market trends in interest rates and various other market factors. Considerations specific to the borrowing institution also affect the maturity and availability of borrowed funds.

External Factors and Exposure to Other Risks

The liquidity needs of a financial institution and the sources of liquidity available to meet those needs depend significantly on the institution's business mix and balance-sheet structure, as well as on the cash-flow profiles of its on- and off-balance-sheet obligations. While management largely determines these internal attributes, external factors and the institution's exposure to various types of financial and operating risks, including interest-rate, credit, operational, legal, and reputational risks, also influence its liquidity profile. As a result, an institution should assess and manage liquidity needs and sources by considering the potential consequences of changes in external factors *along with* the institution-specific determinants of its liquidity profile.

Changes in Interest Rates

The level of prevailing market interest rates, the term structure of interest rates, and changes in both the level and term structure of rates can significantly affect the cash-flow characteristics

and costs of, and an institution's demand for, assets, liabilities, and off-balance-sheet (OBS) positions. In turn, these factors significantly affect an institution's funding structure or liquidity needs, as well as the relative attractiveness or price of alternative sources of liquidity available to it. Changes in the level of market interest rates can also result in the acceleration or deceleration of loan prepayments and deposit flows. The availability of different types of funds may also be affected, as a result of options embedded in the contractual structure of assets, liabilities, and financial transactions.

Economic Conditions

Cyclical and seasonal economic conditions can also have an impact on the volume of an institution's assets, liabilities, and OBS positions—and, accordingly, its cash-flow and liquidity profile. For example, during recessions, business demand for credit may decline, which affects the growth of an organization and its liquidity needs. At the same time, subpar economic growth and its impact on employ-

ment, bankruptcies, and business failures often create direct and indirect incentives for retail customers to reduce their deposits; a recession may also lead to higher loan delinquencies for financial institutions. All of these conditions have negative implications for an institution's cash flow and overall liquidity. On the other hand, periods of economic growth may spur asset or deposit growth, thus introducing different liquidity challenges.

Credit-Risk Exposures of an Institution

An institution's exposure to credit risk can have a material impact on its liquidity. Nonperforming loans directly reduce otherwise expected cash inflows. The reduced credit quality of problem assets impairs their marketability and potential use as a source of liquidity (either by selling the assets or using them as collateral). Moreover, problem assets have a negative impact on overall cash flows by increasing the costs of loan-collection and -workout efforts.

In addition, the price that a bank pays for funds, especially wholesale and brokered borrowed funds and deposits, will reflect the institution's perceived level of risk exposure in the marketplace. Fund suppliers use a variety of credit-quality indicators to judge credit risk and determine the returns they require for the risk to be undertaken. Such indicators include an institution's loan-growth rates; the relative size of its loan portfolio; and the levels of delinquent loans, nonperforming loans, and loan losses. For institutions that have issued public debt, the credit ratings of nationally recognized statistical rating organizations (NRSOs) are particularly critical.

Other Risk Exposures of an Institution

Importantly, exposures to operational, legal, reputational, and other risks can lead to adverse liquidity conditions. Operating risks can materially disrupt the dispersal and receipt of obligated cash flows and give rise to significant liquidity needs. Exposure to legal and reputational risks can lead fund providers to question an institution's overall credit risk, safety and soundness, and ability to meet its obligations in the future. A bank's reputation for operating in a safe and sound manner, particularly its ability to meet its contractual obligations, is an important determinant in its costs of funds and overall liquidity-risk profile.

Given the critical importance of liquidity to financial institutions and the potential impact that other risk exposures and external factors have on liquidity, effective liquidity managers ensure that liquidity management is fully integrated into the institution's overall enterprise-wide risk-management activities. Liquidity management is therefore an important part of an institution's strategic and tactical planning.

Types of Liquidity Risk

Banking organizations encounter the following three broad types of liquidity risk:

- mismatch risk
- market liquidity risk
- contingent liquidity risk

Mismatch risk is the risk that an institution will not have sufficient cash to meet obligations in the normal course of business, as a result of ineffective matches between cash inflows and outflows. The management and control of funding mismatches depend greatly on the daily projections of operational cash flow, including those cash flows that may arise from seasonal business fluctuations, unanticipated new business, and other everyday situations. To accurately project operational cash flows, an institution needs to estimate its expected cash-flow needs and ensure it has adequate liquidity to meet small variations to those expectations. Occurrences of funding mismatches may be frequent. If adequately managed, these mismatches may have little to no impact on the financial health of the firm.

Market liquidity risk is the risk that an institution will encounter market constraints in its efforts to convert assets into cash or to access financial market sources of funds.

The planned conversion of assets into cash is an important element in an institution's ongoing management of funding cash-flow mismatches. In addition, converting assets into cash is often a key strategic tool for addressing contingent liquidity events. As a result, market constraints on achieving planned, strategic, or contingent conversions of assets into cash can exacerbate the severity of potential funding mismatches and contingent liquidity problems.

Contingent liquidity risk is the risk that arises when unexpected events cause an institution to have insufficient funds to meet its obligations. Unexpected events may be firm-specific or arise from external factors. External factors may be geographic, such as local economic factors that affect the premiums required on deposits with certain local, state, or commercial areas, or they may be market-oriented, such as increases in the price volatility of certain types of securities in response to financial market developments. External factors may also be systemic, such as a payment-system disruption or major changes in economic or financial market conditions.

The nature and severity of contingent liquidity events vary substantially. At one extreme, contingent liquidity risk may arise from the need to fund unexpected asset growth as a result of commitment requests or the unexpected runoff of liabilities that occurs in the normal course of business. At the other extreme, institution-specific issues, such as the lowering of a public debt rating or general financial market stress, may have a significant impact on an institution's liquidity and safety and soundness. As a result, managing contingent liquidity risk requires an ongoing assessment of potential future events and circumstances in order to ensure that obligations are met and adequate sources of standby liquidity and/or liquidity reserves are readily available and easily converted to cash.

Diversification plays an important role in managing liquidity and its various component risks. Concentrations in particular types of assets, liabilities, OBS positions, or business activities that give rise to unique types of funding needs or create an undue reliance on specific types of funding sources can unduly expose an institution to the risks of funding mismatches, contingent events, and market liquidity constraints. Therefore, diversification of both the sources and uses of liquidity is a critical component of sound liquidity-risk management.

SOUND LIQUIDITY-RISK MANAGEMENT PRACTICES

Like the management of any type of risk, sound liquidity-risk management involves effective oversight of a comprehensive process that adequately identifies, measures, monitors, and controls risk exposure. This process includes oversight of exposures to funding mismatches, market liquidity constraints, and contingent liquidity events. Both international and U.S. banking supervisors have issued supervisory guidance on safe and sound practices for managing the liquidity risk of banking organizations. Guidance on liquidity risk management was published by the Basel Committee on Banking Supervision, Bank for International Settlements, "Principles for Sound Liquidity Risk Management and Supervision," in September 2008.[1] The U.S. regulatory agencies implemented these principles, jointly agreeing to incorporate those principles into their existing guidance. The revised guidance, "Interagency Policy Statement on Funding and Liquidity Risk Management" was issued on March 10, 2010 (see SR-10-6 and its attachment).

In summary, the critical elements of a sound liquidity-risk management process are—

- Effective corporate governance consisting of oversight by the board of directors and active involvement by management in an institution's control of liquidity risk.
- Appropriate strategies, policies, procedures, and limits used to manage and mitigate liquidity risk.
- Comprehensive liquidity-risk measurement and monitoring systems (including assessments of the current and prospective cash flows or sources and uses of funds) that are commensurate with the complexity and business activities of the institution.
- Active management of intraday liquidity and collateral.
- An appropriately diverse mix of existing and potential future funding sources.
- Adequate levels of highly liquid marketable securities free of legal, regulatory, or operational impediments that can be used to meet liquidity needs in stressful situations.
- Comprehensive contingency funding plans (CFPs) that sufficiently address potential adverse liquidity events and emergency cash flow requirements.
- Internal controls and internal audit processes sufficient to determine the adequacy of the institution's liquidity-risk-management process.

Each of these elements should be customized to account for the sophistication, complexity, and

1. Basel Committee on Banking Supervision, "Principles for Sound Liquidity Risk Management and Supervision," September 2008. See www.bis.org/publ/bcbs144.htm.

business activities of an institution. The following sections discuss supervisory expectations for each of these critical elements.

Corporate Governance and Oversight

Effective liquidity-risk management requires the coordinated efforts of both an informed board of directors and capable senior management. The board should establish and communicate the institution's liquidity-risk tolerance in such a manner that all levels of management clearly understand the institution's approach to managing the trade-offs between management of liquidity risk and short-term profits. The board should ensure that the organizational structures and staffing levels are appropriate, given the institution's activities and the risks they present.

Involvement of the Board of Directors

The board of directors is ultimately responsible for the liquidity risk assumed by the institution. The board should understand and guide the strategic direction of liquidity-risk management. Specifically, the board of directors or a delegated committee of board members should oversee the establishment and approval of liquidity management strategies, policies and procedures, and review them at least annually. In addition, the board should ensure that it

- understands the nature of the institution's liquidity risks and periodically reviews information necessary to maintain this understanding;
- understands and approves those elements of liquidity-risk management policies that articulate the institution's general strategy for managing liquidity risk, and establishes acceptable risk tolerances;
- establishes executive-level lines of authority and responsibility for managing the institution's liquidity risk;
- enforces management's duties to identify, measure, monitor, and control liquidity risk.
- understands and periodically reviews the institution's CFP for handling potential adverse liquidity events; and
- understands the liquidity-risk profile of important subsidiaries and affiliates and their influence on the overall liquidity of the financial institution, as appropriate.

Role of Senior Management

Senior management should ensure that liquidity-risk management strategies, policies, and procedures are adequate for the sophistication and complexity of the institution. Management should ensure that these policies and procedures are appropriately executed on both a long-term and day-to-day basis, in accordance with board delegations. Management should oversee the development and implementation of—

- an appropriate risk-measurement system and standards for measuring the institution's liquidity risk;
- a comprehensive liquidity-risk reporting and monitoring process;
- establishment and monitoring of liquid asset buffers of unencumbered marketable securities;
- effective internal controls and review processes for the management of liquidity risk; and
- monitoring of liquidity risks for each entity across the institution on an on-going basis and;
- an appropriate CFP, including (1) adequate assessments of the institution's contingent liquidity risks under adverse circumstances and (2) fully developed strategies and plans for managing such events.

Senior management should periodically review the organization's liquidity-risk management strategies, policies, and procedures, as well as its CFP, to ensure that they remain appropriate and sound. Management should also coordinate the institution's liquidity-risk management with its efforts for disaster, contingency, and strategic planning, as well as with its business and risk-management objectives, strategies, and tactics. Senior management is also responsible for regularly reporting to the board of directors on the liquidity-risk profile of the institution.

Strategies, Policies, Procedures, and Risk Tolerances

Institutions should have documented strategies for managing liquidity and have formal written policies and procedures for limiting and controlling risk exposures. Strategies, policies, and procedures should translate the board's goals,

objectives, and risk tolerances into operating standards that are well understood by institutional personnel and that are consistent with the board's intended risk tolerances. Policies should also ensure that responsibility for managing liquidity is assigned throughout the corporate structure of the institution, including separate legal entities and relevant operating subsidiaries and affiliates, where appropriate. Strategies set out the institution's general approach for managing liquidity, articulate its liquidity-risk tolerances, and address the extent to which key elements of funds management are centralized or delegated throughout the institution. Strategies also communicate how much emphasis the institution places on using asset liquidity, liabilities, and operating cash flows to meet its day-to-day and contingent funding needs. Quantitative and qualitative targets, such as the following, may also be included in policies:

- guidelines or limits on the composition of assets and liabilities
- the relative reliance on certain funding sources, both on an ongoing basis and under contingent liquidity scenarios
- the marketability of assets to be used as contingent sources of liquidity

An institution's strategies and policies should identify the primary objectives and methods for (1) managing daily operating cash flows, (2) providing for seasonal and cyclical cash-flow fluctuations, and (3) addressing various adverse liquidity scenarios. The latter includes formulating plans and courses of actions for dealing with potential temporary, intermediate-term, and long-term liquidity disruptions. Policies and procedures should formally document—

- lines of authority and responsibility for managing liquidity risk,
- liquidity-risk limits and guidelines,
- the institution's measurement and reporting systems, and
- elements of the institution's comprehensive CFP.

Incorporating these elements of liquidity-risk management into policies and procedures helps internal control and internal audit fulfill their oversight role in the liquidity-risk management process. Policies, procedures, and limits should address liquidity separately for individual currencies, where appropriate and material. All liquidity-risk policies, procedures, and limits should be reviewed periodically and revised as needed.

Delineating Clear Lines of Authority and Responsibility

Through formal written policies or clear operating procedures, management should delineate managerial responsibilities and oversight, including lines of authority and responsibility for the following:

- developing liquidity-risk management policies, procedures, and limits
- developing and implementing strategies and tactics for managing liquidity risk
- conducting day-to-day management of the institution's liquidity
- establishing and maintaining liquidity-risk measurement and monitoring systems
- authorizing exceptions to policies and limits
- identifying the potential liquidity risk associated with the introduction of new products and activities

Institutions should clearly identify the individuals or committees responsible for liquidity-risk decisions. Less complex institutions often assign such responsibilities to the CFO or an equivalent senior management official. Other institutions assign responsibility for liquidity-risk management to a committee of senior managers, sometimes called a finance committee or an asset/liability committee (ALCO). Policies should clearly identify individual or committee duties and responsibilities, the extent of the decision-making authority, and the form and frequency of periodic reports to senior management and the board of directors. In general, an ALCO (or a similar senior-level committee) is responsible for ensuring that (1) measurement systems adequately identify and quantify the institution's liquidity-risk exposure and (2) reporting systems communicate accurate and relevant information about the level and sources of that exposure.

When an institution uses an ALCO or other senior management committee, the committee should actively monitor the liquidity profile of the institution and should have sufficiently broad representation from the major institutional functions that influence liquidity risk (e.g., the lending, investment, deposit, or funding functions).

Committee members should include senior managers who have authority over the units responsible for executing transactions and other activities that can affect liquidity. In addition, the committee should ensure that (1) the risk-measurement system adequately identifies and quantifies risk exposure and (2) the reporting process communicates accurate, timely, and relevant information about the level and sources of risk exposure.

In general, committees overseeing liquidity-risk management delegate the day-to-day responsibilities to the institution's treasury department or, at less complex institutions, to the CFO, treasurer, or other appropriate staff. The personnel charged with measuring and monitoring the day-to-day management of liquidity risk should have a well-founded understanding of all aspects of the institution's liquidity-risk profile. While the day-to-day management of liquidity may be delegated, the oversight committee should not be precluded from aggressively monitoring liquidity management.

In more-complex institutions that have separate legal entities and operating subsidiaries or affiliates, effective liquidity-risk management requires senior managers and other key personnel to have an understanding of the funding position and liquidity of any member of the corporate group that might provide or absorb liquid resources from another member. Centralized liquidity-risk assessment and management can provide significant operating efficiencies and comprehensive views of the liquidity-risk profile of the integrated corporate entity as well as members of the corporate group—including depository institutions. This integrated view is particularly important for understanding the impact other members of the group may have on insured depository entities. However, legal and regulatory restrictions on the flow of funds among members of a corporate group, in addition to differences in the liquidity characteristics and dynamics of managing the liquidity of different types of entities within a group, may call for decentralizing various elements of liquidity-risk management. Such delegation and associated strategies, policies, and procedures should be clearly articulated and understood throughout the organization. Policies, procedures, and limits should also address liquidity separately for individual currencies, legal entities, and business lines, when appropriate and material, as well as allow for legal, regulatory, and operational limits for the transferability of liquidity.

Diversified Funding

An institution should establish a funding strategy that provides effective diversification in the sources and tenor of funding. It should maintain an ongoing presence in its chosen funding markets and strong relationships with funds providers to promote effective diversification of funding sources. An institution should regularly gauge its capacity to raise funds quickly from each source. It should identify the main factors that affect its ability to raise funds and monitor those factors closely to ensure that estimates of fund raising capacity remain valid.

An institution should diversify available funding sources in the short-, medium- and long-term. Diversification targets should be part of the medium- to long-term funding plans and should be aligned with the budgeting and business planning process. Funding plans should take into account correlations between sources of funds and market conditions. Funding should also be diversified across a full range of retail as well as secured and unsecured wholesale sources of funds, consistent with the institution's sophistication and complexity. Management should also consider the funding implications of any government programs or guarantees it utilizes. As with wholesale funding, the potential unavailability of government programs over the intermediate- and long-term should be fully considered in the development of liquidity risk management strategies, tactics, and risk tolerances. Funding diversification should be implemented using limits addressing counterparties, secured versus unsecured market funding, instrument type, securitization vehicle, and geographic market. In general, funding concentrations should be avoided. Undue over reliance on any one source of funding is considered an unsafe and unsound practice.

An essential component of ensuring funding diversity is maintaining market access. Market access is critical for effective liquidity risk management, as it affects both the ability to raise new funds and to liquidate assets. Senior management should ensure that market access is being actively managed, monitored, and tested by the appropriate staff. Such efforts should be consistent with the institution's liquidity-risk profile and sources of funding. For example, access to the capital markets is an important consideration for most large complex institutions, whereas the availability of correspondent lines of credit and other sources of whole funds

are critical for smaller, less complex institutions.

An institution needs to identify alternative sources of funding that strengthen its capacity to withstand a variety of severe institution-specific and market-wide liquidity shocks. Depending upon the nature, severity, and duration of the liquidity shock, potential sources of funding include, but are not limited to, the following:

- Deposit growth.
- Lengthening maturities of liabilities.
- Issuance of debt instruments.
- Sale of subsidiaries or lines of business.
- Asset securitization.
- Sale (either outright or through repurchase agreements) or pledging of liquid assets.
- Drawing-down committed facilities.
- Borrowing.

Liquidity-Risk Limits and Guidelines

Liquidity-risk tolerances or limits should be appropriate for the complexity and liquidity-risk profile of an institution. They should employ both quantitative targets and qualitative guidelines and should be consistent with the institution's overall approach and strategy for measuring and managing liquidity. Policies should clearly articulate a liquidity-risk tolerance that is appropriate for the business strategy of the institution, considering its complexity, business mix, liquidity-risk profile, and its role in the financial system. Policies should also contain provisions for documenting and periodically reviewing assumptions used in liquidity projections. Policy guidelines should employ both quantitative targets and qualitative guidelines. These measurements, limits, and guidelines may be specified in terms of the following measures and conditions, as applicable:

- *Discrete or cumulative cash-flow mismatches or gaps (sources and uses of funds) over specified future short- and long-term time horizons under both expected and adverse business conditions.* Often, these are expressed as cash-flow coverage ratios or as specific aggregate amounts.
- *Target amounts of unpledged liquid-asset reserves sufficient to meet liquidity needs under normal and reasonably anticipated adverse business conditions.* These targets are often expressed as aggregate amounts or as ratios calculated in relation to, for example, total assets, short-term assets, various types of liabilities, or projected-scenario liquidity needs.
- *Volatile liability dependence and liquid-asset coverage of volatile liabilities under both normal and stress conditions.* These guidelines, for example, may include amounts of potentially volatile wholesale funding to total liabilities, volatile retail (e.g., high-cost or out-of-market) deposits to total deposits, potentially volatile deposit-dependency measures, or short-term borrowings as a percent of total funding.
- *Asset concentrations that could increase liquidity risk through a limited ability to convert to cash* (e.g., complex financial instruments, bank-owned (corporate-owned) life insurance, and less-marketable loan portfolios).
- *Funding concentrations that address diversification issues, such as a large liability and dependency on borrowed funds, concentrations of single funds providers, funds providers by market segments, and types of volatile deposit or volatile wholesale funding dependency.* For small community banks, funding concentrations may be difficult to avoid. However, banks that rely on just a few primary sources should have appropriate systems in place to manage the concentrations of funding liquidity, including limit structures and reporting mechanisms.
- *Funding concentrations that address the term, re-pricing, and market characteristics of funding sources.* This may include diversification targets for short-, medium-, and long-term funding, instrument type and securitization vehicles, and guidance on concentrations for currencies and geographical markets.
- *Contingent liabilities, such as unfunded loan commitments and lines of credit supporting asset sales or securitizations, and collateral requirements for derivatives transactions and various types of secured lending.*
- *The minimum and maximum average maturity of different categories of assets and liabilities.*

Institutions may use other risk indicators to specify their risk tolerances. Some institutions may use ratios such as loans to deposits, loans to equity capital, purchased funds to total assets, or other common measures. However, when developing and using such measures, institutions should be fully aware that some measures may not appropriately assess the timing and scenario-specific characteristics of the

institution's liquidity-risk profile. *Liquidity-risk measures that are constructed using static balance-sheet amounts may hide significant liquidity risk that can occur in the future under both normal and adverse business conditions. As a result, institutions should not rely solely on these static measures to monitor and manage liquidity.*

Policies on Measuring and Managing Reporting Systems

Policies and procedures should also identify the methods used to measure liquidity risk, as well as the form and frequency of reports to various levels of management and the board of directors. Policies should identify the nature and form of cash-flow projections and other liquidity measures to be used. Policies should provide for the categorization, measurement, and monitoring of both stable and potentially volatile sources of funds. Policies should also provide guidance on the types of business-condition scenarios used to construct cash-flow projections and should contain provisions for documenting and periodically reviewing the assumptions used in liquidity projections.

Moreover, policies should explicitly provide for more-frequent reporting under adverse business or liquidity conditions. Under normal business conditions, senior managers should receive liquidity-risk reports at least monthly, while the board of directors should receive liquidity-risk reports at least quarterly. If the risk exposure is more complex, the reports should be more frequent. These reports should tell senior management and the board how much liquidity risk the bank is assuming, whether management is complying with risk limits, and whether management's strategies are consistent with the board's expressed risk tolerance.

Policies on Contingency Funding Plans

Policies should also provide for senior management to develop and maintain a written, comprehensive, and up-to-date liquidity CFP. Policies should also ensure that, as part of ongoing liquidity-risk management, senior management is alerted to early-warning indicators or triggers of potential liquidity problems.

Compliance with Laws and Regulations

Institutions should ensure that their policies and procedures take into account compliance with appropriate laws and regulations that can have an impact on an institution's liquidity-risk management and liquidity-risk profile. These laws and regulations include the Federal Deposit Insurance Corporation Improvement Act (FDICIA) and its constraints on an institution's use of brokered deposits, as well as pertinent sections of Federal Reserve regulations A, D, F, and W. (See appendix 2, for a summary of some of the pertinent legal and regulatory issues that should be factored into the management of liquidity risk.)

Liquidity-Risk Measurement Systems

The analysis and measurement of liquidity risk should be tailored to the complexity and risk profile of an institution, incorporating the cash flows and liquidity implications of all the institution's material assets, liabilities, off-balance-sheet positions, and major business activities. Liquidity-risk analysis should consider what effect options embedded in the institution's sources and uses of funds may have on its cash flows and liquidity-risk measures. The analysis of liquidity risk should also be forward-looking and strive to identify potential future funding mismatches as well as current imbalances. Liquidity-risk measures should advance management's understanding of the institution's exposure to mismatch, market, and contingent liquidity risks. Measures should also assess the institution's liquidity sources and needs in relation to the specific business environments it operates in and the time frames involved in securing and using funds.

Adequate liquidity-risk measurement requires the ongoing review of an institution's sources and uses of funds and generally includes analysis of the following:

- trends in balance-sheet structure and funding vehicles
- pro forma cash-flow statements and funding mismatch gaps over varying time horizons
- trends and expectations in the volume and pricing trends for assets, liabilities, and off-balance-sheet items that can have a significant impact on the institution's liquidity

- trends in the relative costs of funds required by existing and alternative funds providers
- the diversification of funding sources and trends in funding concentrations
- the adequacy of asset liquidity reserves, trends in these reserves, and the market dynamics that could influence their market liquidity
- the sensitivity of funds providers to both financial market and institution-specific trends and events
- the institution's exposure to both broad-based market and institution-specific contingent liquidity events

The formality and sophistication of liquidity-risk measurement, and the policies and procedures used to govern the measurement process, depend on the sophistication of the institution, the nature and complexity of its funding structures and activities, and its overall liquidity-risk profile.

(See appendix 1, for background information on the types of liquidity analysis and measures of liquidity risk used by effective liquidity-risk managers. The appendix also discusses the considerations for evaluating the liquidity-risk characteristics of various assets, liabilities, OBS positions, and other activities, such as asset securitization, that can influence an institution's liquidity.)

Pro Forma Cash-Flow Analysis

Regardless of the size and complexity of an institution, pro forma cash-flow statements are a critical tool for adequately managing liquidity risk. In the normal course of measuring and managing liquidity risk and analyzing their institution's sources and uses of funds, effective liquidity managers project cash flows under expected and alternative liquidity scenarios. Such cash-flow-projection statements range from simple spreadsheets to very detailed reports, depending on the complexity and sophistication of the institution and its liquidity-risk profile.

A sound practice is to project, on an ongoing basis, an institution's cash flows under normal business-as-usual conditions, incorporating appropriate seasonal and business-growth considerations over varying time horizons. This cash-flow projection should be regularly reviewed under both short-term and intermediate- to long-term institution-specific contingent scenarios. Institutions that have more-complex liquidity-risk profiles should also assess their exposure to broad systemic and adverse financial market events, as appropriate to their business mix and overall liquidity-risk profile (e.g., securitization, derivatives, trading, processing, international, and other activities).

The construction of pro forma cash-flow statements under alternative scenarios and the ongoing monitoring of an institution's liquidity-risk profile depend importantly on liquidity management's review of trends in the institution's balance-sheet structure and its funding sources. This review should consider past experience and include expectations for the volume and pricing of assets, liabilities, and off-balance-sheet items that may significantly affect the institution's liquidity.

Effective liquidity-risk monitoring systems should assess (1) trends in the relative cost of funds, as required by the institution's existing and alternative funds providers; (2) the diversification or concentration of funding sources; (3) the adequacy of the institution's asset liquidity reserves; and (4) the sensitivity of funds providers to both financial market and institution-specific trends and events. *Detailed examples and further discussion of cash-flows are included in appendix 1, section I, "Basic Cash-Flow Projections."*

Assumptions

Given the critical importance of assumptions in constructing liquidity-risk measures and projections of future cash flows, institutions should ensure that all their assumptions are reasonable and appropriate. Institutions should document and periodically review and approve key assumptions. Assumptions used in assessing the liquidity risk of complex instruments and assets; liabilities; and OBS positions that have uncertain cash flows, market value, or maturities should be subject to rigorous documentation and review.

Assumptions about the stability or volatility of retail deposits, brokered deposits, wholesale or secondary-market borrowings, and other funding sources with uncertain cash flows are particularly important—especially when such assumptions are used to evaluate alternative sources of funds under adverse contingent liquidity scenarios (such as a deterioration in asset quality or capital). When assumptions about the performance of deposits and other sources of

funds are used in the computation of liquidity measures, these assumptions should be based on reasoned analysis considering such factors as the following:

- the historical behavior of deposit customers and funds providers
- how current or future business conditions may change the historical responses and behaviors of customers and other funds providers
- the general conditions and characteristics of the institution's market for various types of funds, including the degree of competition
- the anticipated pricing behavior of funds providers (for instance, wholesale or retail) under the scenario investigated
- haircuts (that is, the reduction from the stated value of an asset) applied to assets earmarked as contingent liquidity reserves

Further discussion of liquidity characteristics of assets, liabilities, and off-balance-sheet items is included in appendix 1, section III, "Liquidity Characteristics of Assets, Liabilities, Off-Balance-Sheet Positions, and Various Types of Banking Activities." Institutions that have complex liquidity profiles should perform sensitivity tests to determine what effect any changes to its material assumptions will have on its liquidity.

Institutions should ensure that assets are properly valued according to relevant financial reporting and supervisory standards. An institution should fully factor into its risk management the consideration that valuations may deteriorate under market stress and take this into account in assessing the feasibility and impact of asset sales on its liquidity position during stress events.

Institutions should ensure that their vulnerabilities to changing liquidity needs and liquidity capacities are appropriately assessed within meaningful time horizons, including intraday, day-to-day, short-term weekly and monthly horizons, medium-term horizons of up to one year, and longer-term liquidity needs over one year. These assessments should include vulnerabilities to events, activities, and strategies that can significantly strain the capability to generate internal cash.

Stress Testing

Once normal operating cash-flow statements are established then those tools can be used to generate stress tests. Stress assumptions are simply layered on top of the normal operating cash-flow projections. The quantitative results provided by the stress test also serve as a key component within the CFP.

Institutions should conduct stress tests on a regular basis for a variety of institution-specific and market-wide events across multiple time horizons. The magnitude and frequency of stress testing should be commensurate with the complexity of the financial institution and the level of its risk exposures. Stress test outcomes should be used to identify and quantify sources of potential liquidity strain and to analyze possible impacts on the institution's cash flows, liquidity position, profitability, and solvency.

Stress tests should also be used to ensure that current exposures are consistent with the financial institution's established liquidity-risk tolerance. The stress test serves as a key component of the CFP and the quantification of the risk to which the institution may be exposed. Management's active involvement and support is critical to the effectiveness of the stress-testing process. Management should discuss the results of stress tests and take remedial or mitigating actions to limit the institution's exposures, build up a liquidity cushion, and adjust its liquidity profile to fit its risk tolerance. The results of stress tests therefore play a key role in determining the amount of buffer assets the institution should maintain.

Cushion of Liquid Assets

Liquid assets are an important source of both primary (operating liquidity) and secondary (contingent liquidity) funding at many institutions. Indeed, a critical component of an institution's ability to effectively respond to potential liquidity stress is the availability of a cushion of highly liquid assets without legal, regulatory, or operational impediments (i.e., unencumbered) that can be sold or pledged to obtain funds in a range of stress scenarios. These assets should be held as insurance against a range of liquidity stress scenarios, including those that involve the loss or impairment of typically available unsecured and/or secured funding sources. The size of the cushion of such high-quality liquid assets should be supported by estimates of liquidity needs performed under an institution's stress testing as well as aligned with the risk tolerance and risk profile of the institution. Management estimates of liquidity needs during periods of

stress should incorporate both contractual and non-contractual cash flows, including the possibility of funds being withdrawn. Such estimates should also assume the inability to obtain unsecured funding as well as the loss or impairment of access to funds secured by assets other than the safest, most liquid assets.

Management should ensure that unencumbered, highly liquid assets are readily available and are not pledged to payment systems or clearing houses. The quality of unencumbered liquid assets is important as it will ensure accessibility during the time of most need. For example, an institution could utilize its holdings of high-quality U.S. Treasury securities, or similar instruments, and enter into repurchase agreements in response to the most severe stress scenarios.

Liquidity-Risk Monitoring and Reporting Systems

Methods used to monitor and measure liquidity risk should be sufficiently robust and flexible to allow for the timely computation of the metrics an institution uses in its ongoing liquidity-risk management. Risk monitoring and reporting systems should regularly provide information on day-to-day liquidity management and risk control; this information should also be readily available during contingent liquidity events.

In keeping with the other elements of sound liquidity-risk management, the complexity and sophistication of management reporting and management information systems (MIS) should be consistent with the liquidity profile of the institution. For example, complex institutions that are highly dependent on wholesale funds may need daily reports on the use of various funding sources, maturities of various instruments, and rollover rates. Less complex institutions may require only simple maturity-gap or cash-flow reports that depict rollovers and mismatch risks; these reports may also include pertinent liquidity ratios. Liquidity-risk reports can be customized to provide management with aggregate information that includes sufficient supporting detail to enable them to assess the sensitivity of the institution to changes in market conditions, its own financial performance, and other important risk factors. Reportable items may include, but are not limited to—

- cash-flow gap-projection reports and forward-looking summary measures that assess both business-as-usual and contingent liquidity scenarios;
- asset and funding concentrations that highlight the institution's dependence on funds that may be highly sensitive to institution-specific contingent liquidity or market liquidity risk (including information on the types and amounts of negotiable certificates of deposit (CDs) and other bank obligations, as well as information on major liquidity funds providers);
- critical assumptions used in cash-flow projections and other measures;
- the status of key early-warning signals or risk indicators;
- funding availability;
- reports on the impact of new products and activities;
- reports documenting compliance with established policies and procedures; and
- where appropriate, both consolidated and unconsolidated reports for institutions that have multiple offices, international branches, affiliates, or subsidiaries.
- Institutions should also report on the use of and availability of government support, such as lending and guarantee programs, and implications on liquidity positions, particularly since these programs are generally temporary or reserved as a source for contingent funding.

The types of reports or information and their timing should be tailored to the institution's funding strategies and will vary according to the complexity of the institution's operations and risk profile. For example, institutions relying on investment securities for their primary source of contingent liquidity should employ reports on the quality, pledging status, and maturity distribution of those assets. Similarly, institutions conducting securitization activities, or placing significant emphasis on the sale of loans to meet contingent liquidity needs, should customize their liquidity reports to target these activities.

Collateral-Position Management

An institution should have the ability to calculate all of its collateral positions in a timely manner, including assets currently pledged relative to the amount of security required and

unencumbered assets available to be pledged. An institution's level of available collateral should be monitored by legal entity, by jurisdiction, and by currency exposure. Systems should be capable of monitoring shifts between intraday and overnight or term-collateral usage. An institution should be aware of the operational and timing requirements associated with accessing the collateral given its physical location (i.e., the custodian institution or securities settlement system with which the collateral is held). Institutions should also fully understand the potential demand on required and available collateral arising from various types of contractual contingencies during periods of both market-wide and institution-specific stress.

Liquidity Across Legal Entities, and Business Lines

An institution should actively monitor and control liquidity-risk exposures and funding needs within and across legal entities and business lines, taking into account legal, regulatory, and operational limitations to the transferability of liquidity. Separately regulated entities will need to maintain liquidity commensurate with their own risk profiles on a stand-alone basis.

Regardless of its organizational structure, it is important that an institution actively monitor and control liquidity risks at the level of individual legal entities, and the group as a whole, incorporating processes that aggregate data across multiple systems in order to develop a group-wide view of liquidity-risk exposures and identify constraints on the transfer of liquidity within the group.

Assumptions regarding the transferability of funds and collateral should be described in liquidity-risk management plans.

Intraday Liquidity Position Management

Intraday liquidity monitoring is an important component of the liquidity-risk management process for institutions engaged in significant payment, settlement, and clearing activities. An institution's failure to manage intraday liquidity effectively, under normal and stressed conditions, could leave it unable to meet payment and settlement obligations in a timely manner, adversely affecting its own liquidity position and that of its counterparties. Among large, complex organizations, the interdependencies that exist among payment systems and the inability to meet certain critical payments has the potential to lead to systemic disruptions that can prevent the smooth functioning of all payment systems and money markets. Therefore, institutions with material payment, settlement and clearing activities should actively manage their intraday liquidity positions and risks to meet payment and settlement obligations on a timely basis under both normal and stressed conditions. Senior management should develop and adopt an intraday liquidity strategy that allows the institution to

- monitor and measure expected daily gross liquidity inflows and outflows.
- manage and mobilize collateral when necessary to obtain intraday credit.
- identify and prioritize time-specific and other critical obligations in order to meet them when expected.
- settle other less critical obligations as soon as possible.
- control credit to customers when necessary.

Contingency Funding Plans

A CFP is a compilation of policies, procedures, and action plans for responding to contingent liquidity events. It is a sound practice for all institutions, regardless of size and complexity, to engage in comprehensive contingent liquidity planning. The objectives of the CFP are to provide a plan for responding to a liquidity crisis, identify a menu of contingent liquidity sources that the institution can use under adverse liquidity circumstances, and describe steps that should be taken to ensure that the institution's sources of liquidity are sufficient to fund scheduled operating requirements and meet the institution's commitments with minimal costs and disruption. CFPs should be commensurate with an institution's complexity, risk profile, and scope of operations.

Contingent liquidity events are unexpected situations or business conditions that may increase the risk that an institution will not have sufficient funds to meet liquidity needs. These events can negatively affect any institution, regardless of its size and complexity, by

- interfering with or preventing the funding of asset growth,

- disrupting the institution's ability to renew or replace maturing funds.

Contingent liquidity events may be institution-specific or arise from external factors. Institution-specific risks are determined by the risk profile and business activities of the institution. They generally are a result of unique credit, market, operational, and strategic risks taken by the institution. A potential result of this type of event would be customers unexpectedly exercising options to withdraw deposits or exercise off-balance-sheet (OBS) commitments.

In contrast, external contingent events may be systemic financial-market occurrences, such as

- increases or decreases in the price volatility of certain types of securities in response to market events;
- major changes in economic conditions, market perception, or dislocations in financial markets;
- disturbances in payment and settlement systems due to operational or local disasters.

Contingent liquidity events range from high-probability/low-impact events that occur during the normal course of business to low-probability/high-impact events that may have an adverse impact on an institution's safety and soundness. Institutions should incorporate planning for high-probability/low-impact liquidity risks into their daily management of the sources and uses of their funds. This objective is best accomplished by assessing possible variations in expected cash-flow projections and provisioning for adequate liquidity reserves in the normal course of business.

Liquidity risks driven by lower-probability, higher-impact events should be addressed in the CFP, which should—

- identify reasonably plausible stress events;
- evaluate those stress events under different levels of severity;
- make a quantitative assessment of funding needs under the stress events;
- identify potential funding sources in response to a stress event; and
- provide for commensurate management processes, reporting, and external communication throughout a stress event.

The CFP should address both the severity and duration of contingent liquidity events. The liquidity pressures resulting from low-probability, high-impact events may be immediate and short term, or they may present sustained situations that have long-term liquidity implications. The potential length of an event should factor into decisions about sources of contingent liquidity.

Identifying Liquidity Stress Events

Stress events are those events that may have a significant impact on an institution's liquidity, given its specific balance-sheet structure, business lines, organizational structure, and other characteristics. Possible stress events include changes in credit ratings, a deterioration in asset quality, a prompt-corrective-action (PCA) downgrade, and CAMELS ratings downgrade widening of credit default spreads, operating losses, negative press coverage, or other events that call into question an institution's ability to meet its obligations.

An institution should customize its CFP. Separate CFPs may be required for the parent company and the consolidated banks in a multibank holding company, for separate subsidiaries (when appropriate), or for each significant foreign currency and global political entity, as necessary. These separate CFPs may be necessary because of legal requirements and restrictions, or the lack thereof. Institutions that have significant payment-system operations should have a formal, written plan in place for managing the risk of both intraday and end-of-day funding failures. Failures may occur as a result of system failure at the institution or at an institution from which payments are expected. Clear, formal communication channels should be established between the institution's operational areas responsible for handling payment-system operations.

Assessing Levels of Severity and Timing

The CFP should delineate the various levels of stress severity that can occur during a contingent liquidity event and, for each type of event, identify the institution's response plan at each stage of an event. (As an event unfolds, it often progresses through various stages and levels of severity.) The events, stages, and severity levels identified should include those that cause temporary disruptions, as well as those that may cause intermediate- or longer-term disruptions.

Institutions can use the different stages or levels of severity to design early-warning indicators, assess potential funding needs at various points during a developing crisis, and specify comprehensive action plans.

Assessing Funding Needs and Sources of Liquidity

A critical element of the CFP is an institution's quantitative projection and evaluation of its expected funding needs and funding capacity during a stress event. The institution should identify the sequence of responses that it will mobilize during a stress event and commit sources of funds for contingent needs well in advance of a stress-related event. To accomplish this objective, the institution needs to analyze potential erosion in its funding at alternative stages or severity levels of the stress event, as well as analyze the potential cash-flow mismatches that may occur during the various stress scenarios and levels. Institutions should base their analyses on realistic assessments of the behavior of funds providers during the event; they should also incorporate alternative contingency funding sources into their plans. The analysis should also include all material on- and OBS cash flows and their related effects, which should result in a realistic analysis of the institution's cash inflows, outflows, and funds availability at different time intervals throughout the potential liquidity stress event—and allow the institution to measure its ability to fund operations over an extended period.

Common tools to assess funding mismatches include

- *Liquidity-gap analysis*—A cash-flow report that essentially represents a base case estimate of where funding surpluses and shortfalls will occur over various future timeframes.
- *Stress tests*—A pro forma cash-flow report with the ability to estimate future funding surpluses and shortfalls under various liquidity stress scenarios and the institution's ability to fund expected asset growth projections or sustain an orderly liquidation of assets under various stress events.

Identify Potential Funding Sources

Because of the potential for liquidity pressures to spread from one source of funding to another during a significant liquidity event, institutions should identify, well in advance, alternative sources of liquidity and ensure that they have ready access to contingent funding sources. These funding sources will rarely be used in the normal course of business. Therefore, institutions should conduct advance planning to ensure that contingent funding sources are readily available. For example, the sale, securitization, or pledging of assets as collateral requires a review of these assets to determine the appropriate haircuts and to ensure compliance with the standards required for executing the strategy. Administrative procedures and agreements should also be in place before the institution needs to access the planned source of liquidity. Institutions should identify what advance steps they need to take to promote the readiness of each of their sources of standby liquidity.

Processes for Managing Liquidity Events

The CFP should identify a reliable crisis-management team and an administrative structure for responding to a liquidity crisis, including realistic action plans executing each element of the plan for each level of a stress event. Frequent communication and reporting among crisis team members, the board of directors, and other affected managers optimizes the effectiveness of a contingency plan by ensuring that business decisions are coordinated to minimize further liquidity disruptions. Effective management of a stress event requires the daily computation of regular liquidity-risk reports and supplemental information. The CFP should provide for more-frequent and more-detailed reporting as a stress situation intensifies. Reports that should be available in a funding crisis include—

- a CD breakage report to identify early redemptions of CDs;
- funding-concentration reports;
- cash-flow projections and run-off reports;
- funding-availability or -capacity reports, by types of funding; and
- reports on the status of contingent funding sources.

Framework for Monitoring Contingent Events

Financial institutions should monitor for potential liquidity stress events by using early-warning indicators and event triggers. These indicators should be tailored to an institution's specific liquidity-risk profile. By recognizing potential stress events early, the institution can proactively position itself into progressive states of readiness as an event evolves. This proactive stance also provides the institution with a framework for reporting or communicating among different institutional levels and to outside parties. Early-warning signals may include but are not limited to—

- rapid asset growth that is funded with potentially volatile liabilities;
- growing concentrations in assets or liabilities;
- negative trends or heightened risk associated with a particular product line;
- rating-agency actions (e.g., agencies watchlisting the institution or downgrading its credit rating);
- negative publicity;
- significant deterioration in the institution's earnings, asset quality, and overall financial condition;
- widening debt or credit-default-swap spreads;
- difficulty accessing longer-term funding;
- increasing collateral margin requirements;
- rising funding costs in a stable market;
- increasing redemptions of CDs before maturity;
- counterparty resistance to OBS products;
- counterparties that begin requesting backup collateral for credit exposures; and
- correspondent banks that eliminate or decrease their credit lines.

To mitigate the potential for reputation contagion when liquidity problems arise, effective communication with counterparties, credit-rating agencies, and other stakeholders is of vital importance. Smaller institutions that rarely interact with the media should have plans in place for how they will manage press inquiries that may arise during a liquidity event. In addition, group-wide CFPs, liquidity cushions, and multiple sources of funding are mechanisms that may mitigate reputation concerns.

In addition to early-warning indicators, institutions that issue public debt, use warehouse financing, securitize assets, or engage in material OTC derivative transactions typically have exposure to event triggers that are embedded in the legal documentation governing these transactions. These triggers protect the investor or counterparty if the institution, instrument, or underlying asset portfolio does not perform at certain predetermined levels. Institutions that rely upon brokered deposits should also incorporate PCA-related downgrade triggers into their CFPs since a change in PCA status could have a material bearing on the availability of this funding source. Contingent event triggers should be an integral part of the liquidity-risk monitoring system.

Asset-securitization programs pose heightened liquidity concerns because an early-amortization event could produce unexpected funding needs. Liquidity contingency plans should address this risk, if it is material to the institution. The unexpected funding needs associated with an early amortization of a securitization event pose liquidity concerns for the originating bank. The triggering of an early-amortization event can result in the securitization trust immediately passing principal payments through to investors. As the holder of the underlying assets, the originating institution is responsible for funding new charges that would normally have been purchased by the trust. Financial institutions that engage in asset securitization should have liquidity contingency plans that address this potential unexpected funding requirement. Management should receive and review reports showing the performance of the securitized portfolio in relation to the early-amortization triggers.[2]

Securitization covenants that cite supervisory thresholds or adverse supervisory actions as triggers for early-amortization events are considered an unsafe and unsound banking practice that undermines the objective of supervisory actions. An early amortization triggered by a supervisory action can create or exacerbate liquidity and earnings problems that can lead to further deterioration in the financial condition of the banking organization.[3]

Securitizations of asset-backed commercial paper programs (ABCPs) are generally supported by a liquidity facility or commitment to purchase assets from the trust if funds are

2. See sections 2130.1, 3020.1, and 4030.1, and the *OCC Handbook on Credit Card Lending*, October 1996.

3. SR-02-14, "Covenants in Securitization Documents Linked to Supervisory Actions or Thresholds."

needed to repay the underlying obligations. Liquidity needs can result from either cash-flow mismatches between the underlying assets and scheduled payments of the overriding security or from credit-quality deterioration of the underlying asset pool. Therefore, the use of liquidity facilities introduces additional risk to the institution, and a commensurate capital charge is required.[4]

Institutions that rely upon secured funding sources also are subject to potentially higher margin or collateral requirements that may be triggered upon the deterioration of a specific portfolio of exposures or the overall financial condition of the institution. The ability of a financially stressed institution to meet calls for additional collateral should be considered in the CFP. Potential collateral values also should be subject to stress tests since devaluations or market uncertainty could reduce the amount of contingent funding that can be obtained from pledging a given asset.

Testing the CFP

Periodic testing of the operational elements of the CFP is an important part of liquidity-risk management. By testing the various operational elements of the CFP, institutions can prevent unexpected impediments or complications in accessing standby sources of liquidity during a contingent liquidity event. It is prudent to test the operational elements of a CFP that are associated with the securitization of assets, repurchase lines, Federal Reserve discount window borrowings, or other borrowings, since efficient collateral processing during a crisis is especially important for such sources. Institutions should carefully consider whether to include unsecured funding lines in their CFPs, since these lines may be unavailable during a crisis.

Larger, more-complex institutions can benefit from operational simulations that test communications, coordination, and decision-making of managers who have different responsibilities, who are in different geographic locations, or who are located at different operating subsidiaries. Simulations or tests run late in the day can highlight specific problems, such as late-day staffing deficiencies or difficulty selling assets or borrowing new funds near the closing time of the financial markets.

Larger, more-complex institutions can benefit from operational simulations that test communications, coordination, and decisionmaking of managers who have different responsibilities, who are in different geographic locations, or who are located at different operating subsidiaries. Simulations or tests run late in the day can highlight specific problems, such as late-day staffing deficiencies or difficulty selling assets or borrowing new funds near the closing time of the financial markets.

Internal Controls

An institution's internal controls consist of policies, procedures, approval processes, reconciliations, reviews, and other types of controls to provide assurances that the institution manages liquidity risk in accordance with the board's strategic objectives and risk tolerances. Appropriate internal controls should address relevant elements of the risk-management process, including the institution's adherence to polices and procedures; the adequacy of its risk identification, risk measurement, and risk reporting; and its compliance with applicable rules and regulations. The results of reviews of the liquidity-risk management process, along with any recommendations for improvement, should be reported to the board of directors, which should take appropriate and timely action.

An important element of a bank's internal controls is management's comprehensive evaluation and review. Management should ensure that an independent party regularly reviews and evaluates the components of the institution's liquidity-risk management process. These reviews should assess the extent to which the institution's liquidity-risk management complies with both supervisory guidance and industry sound practices, taking into account the level of sophistication and complexity of the institution's liquidity-risk profile. In larger, complex institutions, an internal audit function usually performs this review. Smaller, less complex institutions may assign the responsibility for conducting an independent evaluation and review to qualified individuals who are independent of the function they are assigned to review. The independent review should report key issues requiring attention, including

4. SR-05-13, "Interagency Guidance on the Eligibility of ABCP Liquidity Facilities and the Resulting Risk-Based Capital Treatment."

instances of noncompliance, to the appropriate level of management to initiate a prompt correction of the issues, consistent with approved policies.

Periodic reviews of the liquidity-risk management process should address any significant changes that have occurred since the last review, such as changes in the institution's types or characteristics of funding sources, limits, and internal controls. Reviews of liquidity-risk measurement systems should include assessments of the assumptions, parameters, and methodologies used. These reviews should also seek to understand, test, and document the current risk-measurement process; evaluate the system's accuracy; and recommend solutions to any identified weaknesses.

Controls for changes to the assumptions the institution uses to make cash-flow projections should require that the assumptions not be altered without clear justification consistent with approved strategies. The name of the individual authorizing the change, along with the date of the change, the nature of the change, and justification for each change, should be fully documented. Documentation for all assumptions used in cash-flow projections should be maintained in a readily accessible, understandable, and auditable form. Because liquidity-risk measurement systems may incorporate one or more subsidiary systems or processes, institutions should ensure that multiple component systems are well integrated and consistent with each other.

LIQUIDITY-RISK MANAGEMENT FOR BANK HOLDING COMPANIES

Bank holding companies (BHCs) should develop and maintain liquidity-risk management processes and funding programs that are consistent with their level of sophistication and complexity. For BHCs (includes financial holding companies, which are BHCs) see the *Bank Holding Company Supervision Manual*, section 4066, *"Funding and Liquidity Risk Management,"* and sections 1050.0 and 1050.1, that discuss the consolidated supervision of BHCs. See also SR-10-6, "Interagency Policy Statement on Funding and Liquidity Risk Management." Also see sections 4010.0, "Parent Only—Debt Servicing Capacity/Cash Flow" and 4010.2 "Parent Only—Liquidity."

SUPERVISORY PROCESS FOR EVALUATING LIQUIDITY RISK

Liquidity risk is a primary concern for all banking organizations and is an integral component of the CAMELS rating system. Examiners should consider liquidity risk during the preparation and performance of all on-site safety-and-soundness examinations as well as during targeted supervisory reviews. To meet examination objectives efficiently and effectively and remain sensitive to potential burdens imposed on institutions, examiners should follow a structured, risk-focused approach for the examination of liquidity risk. Key elements of this examination process include off-site monitoring and a risk assessment of the institution's liquidity-risk profile. These elements will help the examiner develop an appropriate plan and scope for the on-site examination, thus ensuring the exam is as efficient and productive as possible. A fundamental tenet of the risk-focused examination approach is the targeting of supervisory resources at functions, activities, and holdings that pose the most risk to the safety and soundness of an institution.

For smaller institutions that have less complex liquidity profiles, stable funding sources, and low exposures to contingent liquidity circumstances, the liquidity element of an examination may be relatively simple and straightforward. On the other hand, if an institution is experiencing significant asset and product growth; is highly dependent on potentially volatile funds; or has a complex business mix, balance-sheet structure, or liquidity-risk profile that exposes the institution to contingent liquidity risks, that institution should generally receive greater supervisory attention. Given the contingent nature of liquidity risk, institutions whose corporate structure gives rise to inherent operational risk, or institutions encountering difficulties associated with their earnings, asset quality, capital adequacy, or market sensitivity, should be especially targeted for review of the adequacy of their liquidity-risk management.

Off-Site Risk Assessment

In off-site monitoring and analysis, a preliminary view, or *risk assessment*, is developed before initiating an on-site examination. Both the inherent level of an institution's liquidity-

risk exposure and the quality of its liquidity-risk management should be assessed to the fullest extent possible during the off-site phase of the examination process. The following information can be helpful in this assessment:

- organizational charts and policies that identify authorities and responsibilities for managing liquidity risk
- liquidity policies, procedures, and limits
- ALCO committee minutes and reports (minutes and reports issued since the last examination or going back at least six to twelve months before the examination)
- board of directors reports on liquidity-risk exposures
- audit reports (both internal and external)
- other available internal liquidity-risk management reports, including cash-flow projections that detail key assumptions
- internal reports outlining funding concentrations, the marketability of assets, analysis that identifies the relative stability or volatility of various types of liabilities, and various cash-flow coverage ratios projected under adverse liquidity scenarios
- supervisory surveillance reports and supervisory screens
- external public debt ratings (if available)

Quantitative liquidity exposure should be assessed by conducting as much of the supervisory review off-site as practicable. This off-site work includes assessing the bank's overall liquidity-risk profile and the potential for other risk exposures, such as credit, market, operational, legal, and reputational risks, that may have a negative impact on the institution's liquidity under adverse circumstances. These assessments can be conducted on a preliminary basis using supervisory screens, examiner-constructed measures, internal bank measures, and cash-flow projections obtained from management reports received before the on-site engagement. Additional factors to be incorporated in the off-site risk assessment include the institution's balance-sheet composition and the existence of funding concentrations, the marketability of its assets (in the context of liquidation, securitization, or use of collateral), and the institution's access to secondary markets of liquidity.

The key to assessing the quality of management is an organized discovery process aimed at determining whether appropriate corporate-governance structures, policies, procedures, limits, reporting systems, CFPs, and internal controls are in place. This discovery process should, in particular, ascertain whether all the elements of sound liquidity-risk management are applied consistently. The results and reports of prior examinations, in addition to internal management reports, provide important information about the adequacy of the institution's risk management.

Examination Scope

The off-site risk assessment provides the examiner with a preliminary view of both the adequacy of liquidity management and the magnitude of the institution's exposure. The scope of the on-site liquidity-risk examination should be designed to confirm or reject the off-site hypothesis and should target specific areas of interest or concern. In this way, on-site examination procedures are tailored to the institution's activities and risk profile and use flexible and targeted work-documentation programs. In general, if liquidity-risk management is identified as adequate, examiners can rely more heavily on a bank's internal liquidity measures for assessing its inherent liquidity risk.

The examination scope for assessing liquidity risk should be commensurate with the complexity of the institution and consistent with the off-site risk assessment. For example, only baseline examination procedures would be used for institutions whose off-site risk assessment indicates that they have adequate liquidity-risk management processes and low levels of inherent liquidity exposure. These institutions include those that have noncomplex balance-sheet structures and banking activities and that also meet the following criteria:

- well capitalized; minimal issues with asset quality, earnings, and market-risk-sensitive activities
- adequate reserves of marketable securities that can serve as standby sources of liquidity
- minimal funding concentrations
- funding structures that are principally composed of stable liabilities
- few OBS items, such as loan commitments, that represent contingent liquidity draws
- minimal potential exposure to legal and reputational risk

- formal adoption of well-documented liquidity-management policies, procedures, and CFPs

For these and other institutions identified as potentially low risk, the scope of the on-site examination would consist of only those examination procedures necessary to confirm the risk-assessment hypothesis. The adequacy of liquidity-risk management could be verified through a basic review of the appropriateness of the institution's policies, internal reports, and controls and its adherence to them. The integrity and reliability of the information used to assess the quantitative level of risk could be confirmed through limited sampling and testing. In general, if basic examination procedures validate the risk assessment, the examiner may conclude the examination process.

High levels of inherent liquidity risk may arise if an institution has concentrations in specific business activities, products, and sectors, or if it has balance-sheet risks, such as unstable liabilities, risky assets, or planned asset growth without an adequate plan for funding the asset growth. OBS items that have uncertain cash inflows may also be a source of inherent liquidity risk. Institutions for which a risk assessment indicated high levels of inherent liquidity-risk exposure and strong liquidity management may require a more extensive examination scope to confirm the assessment. These expanded procedures may entail more analysis of the institution's liquidity-risk measurement system and its liquidity-risk profile. When high levels of liquidity-risk exposure are found, examiners should focus special attention on the sources of this risk. When a risk assessment indicates an institution has high exposure and weak risk-management systems, an extensive work-documentation program is required. The institution's internal measures should be used cautiously, if at all.

Regardless of the sophistication or complexity of an institution, examiners must use care during the on-site phase of an examination to confirm the off-site risk assessment and identify issues that may have escaped off-site analysis. Accordingly, the examination scope should be adjusted as on-site findings dictate.

Assessing CAMELS "L" Ratings

The assignment of the "L" rating is integral to the CAMELS ratings process for commercial banks. Examination findings on both (1) the inherent level of an institution's liquidity risk and (2) the adequacy of its liquidity-risk management process should be incorporated in the assignment of the "L" rating. Findings on the adequacy of liquidity-risk management should also be reflected in the CAMELS "M" rating for risk management.

Examiners can develop an overall assessment of an institution's liquidity-risk exposure by reviewing the various characteristics of its assets, liabilities, OBS instruments, and material business activities. An institution's asset credit quality, earnings integrity, and market risk may also have significant implications for its liquidity-risk exposure. Importantly, assessments of the adequacy of an institution's liquidity-management practices may affect the assessment of its inherent level of liquidity risk. For institutions judged to have sound and timely liquidity-risk measurement and reporting systems and CFPs, examiners may use the results of the institution's adverse-scenario cash-flow projections in order to gain insight into its level of inherent exposure. Institutions that have less-than-adequate measurement and reporting systems and CFPs may have higher exposure to liquidity risk as a result of their potential inability to respond to adverse liquidity events.

Elements of strong liquidity-risk management are particularly important during stress events and include many of the items discussed previously: communication among the departments responsible for managing liquidity, reports that indicate a diversity of funding sources, standby funding sources, cash-flow analyses, liquidity stress tests, and CFPs. Liquidity-risk management should also manage the ongoing costs of maintaining liquidity.

Liquidity risk should be rated in accordance with the Uniform Financial Institutions Rating System (UFIRS).[5] The assessment of the adequacy of liquidity-risk management should provide the primary basis for reaching an overall assessment on the "L" component rating since it is a leading indicator of potential liquidity-risk exposure. Accordingly, overall ratings for liquidity-risk sensitivity should be no greater

5. SR-96-38, "Uniform Financial Institutions Rating System" and section A.5020.1.

than the rating given to liquidity-risk management.

In evaluating the adequacy of a financial institution's liquidity position, consideration should be given to the current level and prospective sources of liquidity compared with funding needs, as well as to the adequacy of funds-management practices relative to the institution's size, complexity, and risk profile. In general, funds-management practices should ensure that an institution is able to maintain a level of liquidity sufficient to meet its financial obligations in a timely manner and to fulfill the legitimate banking needs of its community. Practices should reflect the ability of the institution to manage unplanned changes in funding sources, as well as react to changes in market conditions that affect the ability to quickly liquidate assets with minimal loss. In addition, funds-management practices should ensure that liquidity is not maintained at a high cost or through undue reliance on funding sources that may not be available in times of financial stress or adverse changes in market conditions.

Liquidity is rated based upon, but not limited to, an assessment of the following evaluation factors:

- the adequacy of liquidity sources compared with present and future needs and the ability of the institution to meet liquidity needs without adversely affecting its operations or condition
- the availability of assets readily convertible to cash without undue loss
- access to money markets and other sources of funding
- the level of diversification of funding sources, both on- and off-balance-sheet
- the degree of reliance on short-term, volatile sources of funds, including borrowings and brokered deposits, to fund longer-term assets
- the trend and stability of deposits
- the ability to securitize and sell certain pools of assets
- the capability of management to properly identify, measure, monitor, and control the institution's liquidity position, including the effectiveness of funds-management strategies, liquidity policies, management information systems, and CFPs

Ratings of liquidity-risk management should follow the general framework used to rate overall risk management:

- A rating of 1 indicates strong liquidity levels and well-developed funds-management practices. The institution has reliable access to sufficient sources of funds on favorable terms to meet present and anticipated liquidity needs.
- A rating of 2 indicates satisfactory liquidity levels and funds-management practices. The institution has access to sufficient sources of funds on acceptable terms to meet present and anticipated liquidity needs. Modest weaknesses may be evident in funds-management practices.
- A rating of 3 indicates liquidity levels or funds-management practices in need of improvement. Institutions rated 3 may lack ready access to funds on reasonable terms or may evidence significant weaknesses in funds-management practices.
- A rating of 4 indicates deficient liquidity levels or inadequate funds-management practices. Institutions rated 4 may not have or be able to obtain a sufficient volume of funds on reasonable terms to meet liquidity needs.
- A rating of 5 indicates liquidity levels or funds-management practices so critically deficient that the continued viability of the institution is threatened. Institutions rated 5 require immediate external financial assistance to meet maturing obligations or other liquidity needs.

Unsafe liquidity-risk exposures and weaknesses in managing liquidity risk should be fully reflected in the overall liquidity-risk ratings. Unsafe exposures and unsound management practices that are not resolved during the on-site examination should be addressed through subsequent follow-up actions by the examiner and other supervisory personnel.

REFERENCES

The following sources provide additional information on liquidity-risk management:

- *Bank Holding Company Supervision Manual*, Board of Governors of the Federal Reserve System.
- Basel Committee on Banking Supervision, "Sound Practices for Managing Liquidity in Banking Organisations," publication 69, February 2000.
- "Determining Conformance With Interest Rate

Restrictions for Less Than Well Capitalized Institutions,'' Federal Deposit Insurance Corporation, November 3, 2009 (FIL 62-2009)
- Federal Deposit Insurance Corporation, *Risk Management Manual of Examination Policies*, section 6.1—''Liquidity and Funds Management.''
- Federal Financial Institutions Examination Council, Uniform Bank Performance Report.
- Interagency Policy Statement on Funding and Liquidity Risk Management, March 17, 2010
- Office of the Comptroller of the Currency, *Comptroller's Handbook (Safety & Soundness)*, ''Liquidity,'' February 2001.
- ''Process for Determining If An Institution Subject to Interest-Rate Restrictions is Operating in a High-Rate Area,'' Federal Deposit Insurance Corporation, December 4, 2009 (FIL 69-2009)
- SR-01-08, ''Supervisory Guidance on Complex Wholesale Borrowings,'' Board of Governors of the Federal Reserve System, April 5, 2001.
- SR-01-14, ''Joint Agency Advisory on Rate-Sensitive Deposits,'' Board of Governors of the Federal Reserve System, May 31, 2001.
- SR-03-15, ''Interagency Advisory on the Use of the Federal Reserve's Primary Credit Program in Effective Liquidity Management,'' Board of Governors of the Federal Reserve System, July 25, 2003.
- SR-10-6, ''Interagency Policy Statement on Funding and Liquidity-Risk Management,'' Board of Governors of the Federal Reserve System, March 17, 2010.
- *Trading and Capital-Markets Activities Manual*, Board of Governors of the Federal Reserve System.

APPENDIX 1—FUNDAMENTALS OF LIQUIDITY-RISK MEASUREMENT

Measuring a financial institution's liquidity-risk profile and identifying alternative sources of funds to meet cash-flow needs are critical elements of sound liquidity-risk management. The liquidity-measurement techniques and the liquidity measures employed by depository institutions vary across a continuum of granularity, specificity, and complexity, depending on the specific characteristics of the institution and the intended users of the information. At one extreme, highly granular cash-flow projections under alternative scenarios are used by both complex and noncomplex firms to manage their day-to-day funding mismatches in the normal course of business and for assessing their contingent liquidity-risk exposures. At the other end of the measurement spectrum, aggregate measures and various types of liquidity ratios are often employed to convey summary views of an institution's liquidity-risk profile to various levels of management, the board of directors, and other stakeholders. As a result of this broad continuum, effective managers generally use a combination of cash-flow analysis and summary liquidity-risk measures in managing their liquidity-risk exposures, since no one measure or measurement technique can adequately capture the full dynamics of a financial institution's liquidity-risk exposure.

This appendix provides background material on the basic elements of liquidity-risk measurement and is intended to enhance examiners' understanding of the key elements of liquidity-risk management. First, the fundamental structure of cash-flow-projection worksheets and their use in assessing cash-flow mismatches under both normal business conditions and contingent liquidity events are discussed. The appendix then discusses the key liquidity characteristics of common depository institution assets, liabilities, off-balance-sheet (OBS) items, and other activities. These discussions also present key management considerations surrounding various sources and uses of liquidity in constructing cash-flow worksheets and addressing funding gaps under both normal and adverse conditions. Finally, commonly used summary liquidity measures and ratios are discussed, along with special considerations that should enter into the construction and use of these summary measures.[6]

I. Basic Cash-Flow Projections

In measuring an institution's liquidity-risk profile, effective liquidity managers estimate cash inflows and cash outflows over future periods. For day-to-day operational purposes, cash-flow projections for the next day and subsequent days

6. Material presented in this appendix draws from the OCC *Liquidity Handbook*, FDIC guidance, Federal Reserve guidance, findings from Federal Reserve supervision reviews, and other material developed for the Federal Reserve by consultants and other outside parties.

out over the coming week are used in order to ensure that contractual obligations are met on time. Such daily projections can be extended out beyond a one-week horizon, although it should be recognized that the further out such projections are made, the more susceptible they become to error arising from unexpected changes.

For planning purposes, effective liquidity managers project cash flows out for longer time horizons, employing various incremental time periods, or "buckets," over a chosen horizon. Such buckets may encompass forward weeks, months, quarters, and, in some cases, years. For example, an institution may plan its cash inflows and outflows on a daily basis for the next 5–10 business days, on a weekly basis over the coming month or quarter, on a monthly basis over the coming quarter or quarters, and on a quarterly basis over the next half-year or year. Such cash-flow bucketing is usually compiled into a single cash-flow-projection worksheet or report that represents cash flows under a specific future scenario. The goal of this bucketing approach is a measurement system with sufficient granularity to (1) reveal the time dimension of the needs and sources of liquidity and (2) identify potential liquidity-risk exposure to contingent events.

In its most basic form, a cash-flow-projection worksheet is a table with columns denoting the selected time periods or buckets for which cash flows are to be projected. The rows of this table consist of various types of assets, liabilities, and OBS items, often grouped by their cash-flow characteristics. Different groupings may be used to achieve different objectives of the cash-flow projection. For each row, net cash flows arising from the particular asset, liability, or OBS activity are projected across the time buckets.

The detail and granularity of the rows, and thus the projections, depend on the sophistication and complexity of the institution. Complex banks generally favor more detail, while less complex banks may use higher levels of aggregation. Static projections based only on the contractual cash flows of assets, liabilities, and OBS items as of a point in time are helpful for identifying gaps between needs and sources of liquidity. However, static projections may inadequately quantify important aspects of potential liquidity risk because they ignore new business, funding renewals, customer options, and other potential events that may have a significant impact on the institution's liquidity profile. Since liquidity managers are generally interested in evaluating how available liquidity sources may cover both expected and potential unexpected liquidity needs, a dynamic analysis that includes management's projected changes in cash flows is normally far more useful than a static projection based only on contractual cash flows as of a given projection date.

In developing a cash-flow-projection worksheet, cash inflows occurring within a given time horizon or time bucket are represented as positive numbers, while outflows are represented as negative numbers. Cash inflows include increases in liabilities as well as decreases in assets, and cash outflows include decreases in liabilities as well as increases in assets. For each type of asset, liability, or OBS item, and in each time bucket, the values shown in the cells of the projected worksheet are net cash-flow numbers. One format for a cash-flow-projection worksheet arrays sources of net cash inflows (such as loans and securities) in one group and sources of net cash outflows (such as deposit runoffs) in another. For example, the entries across time buckets for a loan or loan category would net the positives (cash inflows) of projected interest, scheduled principal payments, and prepayments with the negatives (cash outflows) of customer draws on existing commitments and new loan growth in each appropriate time bucket. Summing the net cash flows within a given column or time bucket identifies the extent of maturity mismatches that may exist. Funding shortfalls caused by mismatches in particular time frames are revealed as a "negative gap," while excess funds within a time bucket denote a "positive gap." Identifying such gaps early can help managers take the appropriate action to either fill a negative gap or reduce a positive gap. The subtotals of the net inflows and net outflows may also be used to construct net cash-flow coverage ratios or the ratio of net cash inflows to net cash outflows.

The specific worksheet formats used to array sources and uses of cash can be customized to achieve multiple objectives. Exhibit 1 provides an example of one possible form of a cash-flow-projection worksheet. The time buckets (columns) and sources and uses (rows) are selected for illustrative purposes, as the specific selection will depend on the purpose of the particular cash-flow projection. In this example, assets and liabilities are grouped into two broad categories: those labeled "customer-driven cash flows" and those labeled "management-controlled cash flows." This grouping arrays projected cash

Exhibit 1—Example Cash-Flow-Projection Worksheet

	Day 1	*Week 1*	*Week 2*	*Week 3*	*Month 1*	*Month 3*	*Months 4–6*	*Months 7–12*
Customer-driven cash flows								
Consumer loans								
Business loans								
Residential mortgage loans								
Fixed assets								
Other assets								
Noninterest-bearing deposits								
NOW accounts								
MMDAs								
Passbook savings								
Statement savings								
CDs under $100,000								
Jumbo CDs								
Net noninterest income								
Miscellaneous and other liabilities								
Other								
Subtotal								
Management-controlled cash flows								
Investment securities								
Repos, FFP, & other short-term borrowings								
FHLB & other borrowings								
Committed lines								
Uncommitted lines								
Other								
Subtotal								
Net cash-flow gap								
Cumulative position								

flows on the basis of the relative extent to which funding managers may have control over changes in the cash flows of various assets, liabilities, OBS items, and other activities that have an impact on cash flow. For example, managers generally have less control over loan and deposit cash flows (e.g., changes arising from either growth or attrition) and more control over such items as fed funds sold, investment securities, and borrowings.

The net cash-flow gap illustrated in the next-to-the-last row of exhibit 1 is the sum of the net cash flows in each time-bucket column and reflects the funding gap that will have to be financed in that time period. For the daily time buckets, this gap represents the net overnight position that needs to be funded in the unsecured short-term (e.g., fed funds) market. The final row of the exhibit identifies a cumulative net cash-flow gap, which is constructed as the sum of the net cash flows in that particular time bucket and all previous time buckets. It provides a running picture across time of the cumulative funding sources and needs of the institution. The worksheet presented in exhibit 1 is only one of many alternative formats that can be used in measuring liquidity gaps.

II. Scenario Dependency of Cash-Flow Projections

Cash-flow-projection worksheets describe an institution's liquidity profile under an estab-

lished set of assumptions about the future.

The set of assumptions used in the cash-flow projection constitutes a specific scenario customized to meet the liquidity manager's objective for the forecast. Effective liquidity managers generally use multiple forecasts and scenarios to achieve an array of objectives over planning time horizons. For example, they may use three broad types of scenarios every time they make cash-flow projections: normal-course-of-business scenarios; short-term, institution-specific stress scenarios; and more-severe, intermediate-term, institution-specific stress scenarios. Larger, more complex institutions that engage in significant capital-markets and derivatives activities also routinely project cash flows for various systemic scenarios that may have an impact on the firm. Each scenario requires the liquidity manager to assess and plan for potential funding shortfalls. Importantly, no single cash-flow projection reflects the range of liquidity sources and needs required for advance planning.

Normal-course-of-business scenarios establish benchmarks for the "normal" behavior of cash flows of the institution. The cash flows projected for such scenarios are those the institution expects under benign conditions and should reflect seasonal fluctuations in loans or deposit flows. In addition, expected growth in assets and liabilities is generally incorporated to provide a dynamic view of the institution's liquidity needs under normal conditions.

Adverse, institution-specific scenarios are those that subject the institution to constrained liquidity conditions. Such scenarios are generally defined by first specifying the type of liquidity event to be considered and then identifying various levels or stages of severity for that type of event. For example, institutions that do not have publicly rated debt generally employ scenarios that entail a significant deterioration in the credit quality of their loan and security holdings. Insitutions that have publicly rated debt generally include a debt-rating downgrade scenario in their CFPs. The downgrade of an institution's public debt rating might be specified as one type of event, with successively lower ratings grades, including below-investment-grade ratings, to identify increasing levels of severity. Each level of severity can be viewed as an individual scenario for planning purposes. Effective liquidity managers ensure that they choose potential adverse liquidity scenarios that entail appropriate degrees of severity and model cash flows consistent with each level of stress. Events that limit access to important sources of funding are the most common institution-specific scenarios used.

The same type of cash-flow-projection worksheet format shown in exhibit 1 can be used for adverse, institution-specific scenarios. However, in making such cash-flow projections, some institutions find it useful to organize the accounts differently to accommodate a set of very different assumptions from those used in the normal-course-of-business scenarios. Exhibit 2 presents a format in which accounts are organized by those involving potential cash outflows and cash inflows. This format focuses the analysis first on liability erosion and potential off-balance-sheet draws, followed by an evaluation of the bank's ability to cover potential runoff, primarily from assets that can be sold or pledged. Funding sources are arranged by their sensitivity to the chosen scenario. For example, deposits may be segregated into insured and uninsured portions. The time buckets used are generally of a shorter term than those used under business-as-usual scenarios, reflecting the speed at which deteriorating conditions can affect cash flows.

A key goal of creating adverse-situation cash-flow projections is to alert management as to whether incremental funding resources available under the constraints of each scenario are sufficient to meet the incremental funding needs that result from that scenario. To the extent that projected funding deficits are larger than (or projected funding surpluses are smaller than) desired levels, management has the opportunity to adjust its liquidity position or develop strategies to bring the institution back within an acceptable level of risk.

Adverse systemic scenarios entail macroeconomic, financial market, or organizational events that can have an adverse impact on the institution and its funding needs and sources. Such scenarios are generally customized to the individual institution's funding characteristics and business activities. For example, an institution involved in clearing and settlement activities may choose to model a payments-system disruption, while a bank heavily involved in capital-markets transactions may choose to model a capital-markets disruption.

The number of cash-flow projections necessary to fully assess potential adverse liquidity scenarios can result in a wealth of information that often requires summarization in order to appropriately communicate contingent liquidity-risk exposure to various levels of management.

Exhibit 2—Example Cash-Flow-Projection Worksheet—Liquidity Under an Adverse Scenario

Potential outflows/funding erosion	*Day 1*	*Day 2*	*Days 3–7*	*Week 2*	*Week 3*	*Week 4*	*Month 2*	*Months 2+*
Federal funds purchased								
Uncollateralized borrowings (sub-debt, MTNs, etc.)								
Nonmaturity deposits: insured								
— Noninterest-bearing deposits								
— NOW accounts								
— MMDAs								
— Savings								
Nonmaturity deposits: uninsured								
— Retail CDs under $100,000								
— Jumbo CDs								
— Brokered CDs								
— Miscellaneous and other liabilities								
Subtotal								
Off-balance-sheet funding requirements								
Loan commitments								
Amortizing securitizations								
Out-of-the-money derivatives								
Backup lines								
Total potential outflows								
Potential sources to cover outflows								
Overnight funds sold								
Unencumbered investment securities (with appropriate haircut)								
Residential mortgage loans								
Consumer loans								
Business loans								
Fixed/other assets								
Unsecured borrowing capacity								
Brokered-funds capacity								
Total potential inflows								
Net cash flows								
Coverage ratio (inflows/outflows)								
Cumulative coverage ratio								

Exhibit 3—Example Summary Contingent-Liquidity-Exposure Report (for an Assumed Time Horizon)

Events:	*Current*	*Ratings downgrade*		*Earnings*	*Reputation*	*Other (?)*
Scenarios:		*1 category*	*BBB to BB*	*RoA = ?*		
Potential funding erosion						
Large fund providers	___	___	___	___	___	___
Fed funds	___	___	___	___	___	___
CDs	___	___	___	___	___	___
Eurotakings/foreign deposits	___	___	___	___	___	___
Commercial paper	___	___	___	___	___	___
Subtotal	___	___	___	___	___	___
Other funds providers						
Fed funds	___	___	___	___	___	___
CDs	___	___	___	___	___	___
Eurotakings/foreign deposits	___	___	___	___	___	___
Commercial paper	___	___	___	___	___	___
DDAs	___	___	___	___	___	___
Consumer						
MMDAs	___	___	___	___	___	___
Savings	___	___	___	___	___	___
Other	___	___	___	___	___	___
Total uninsured funds	___	___	___	___	___	___
Total insured funds	___	___	___	___	___	___
Total funding	___	___	___	___	___	___
Off-balance-sheet needs						
Letters of credit	___	___	___	___	___	___
Loan commitments	___	___	___	___	___	___
Securitizations	___	___	___	___	___	___
Derivatives	___	___	___	___	___	___
Total OBS items	___	___	___	___	___	___
Total funding erosion	___	___	___	___	___	___
Sources of funds						
Surplus money market	___	___	___	___	___	___
Unpledged securities	___	___	___	___	___	___
Securitizations						
Credit cards	___	___	___	___	___	___
Autos	___	___	___	___	___	___
Mortgages	___	___	___	___	___	___
Loan sales	___	___	___	___	___	___
Other	___	___	___	___	___	___
Total internal sources	___	___	___	___	___	___
Borrowing capacity	___	___	___	___	___	___
Brokered-funds capacity	___	___	___	___	___	___
Fed discount borrowings	___	___	___	___	___	___
Other	___	___	___	___	___	___

Exhibit 3 presents an example of a report format that assesses available sources of liquidity under alternative scenarios. The worksheet shows the amount of anticipated funds erosion and potential sources of funds under a number of stress scenarios, for a given time bucket (e.g., overnight, one week, one month, etc.). In this example, two rating-downgrade scenarios of different severity are used, along with a scenario built on low-earnings projections and a potential reputational-risk scenario.

Exhibit 4 shows an alternative format for summarizing the results of multiple scenarios. In this case, summary funding gaps are presented across various time horizons (columns) for each scenario (rows). Actual reports used should be tailored to the specific liquidity-risk profile and other institution-specific characteristics.

III. Liquidity Characteristics of Assets, Liabilities, Off-Balance-Sheet Positions, and Various Types of Banking Activities

A full understanding of the liquidity and cash-flow characteristics of the institution's assets, liabilities, OBS items, and banking activities is critical to the identification and management of mismatch risk, contingent liquidity risk, and market liquidity risk. This understanding is required for constructing meaningful cash-flow-projection worksheets under alternative scenarios, for developing and executing strategies used in managing mismatches, and for customizing summary liquidity measures or ratios.

A. Assets

The generation of assets is one of the primary uses of funds at banking organizations. Once acquired, assets provide cash inflows through principal and interest payments. Moreover, the liquidation of assets or their use as collateral for borrowing purposes makes them an important source of funds and, therefore, an integral tool in managing liquidity risk. As a result, the objectives underlying an institution's holdings of various types of assets range along a continuum that balances the tradeoffs between maximizing risk-adjusted returns and ensuring the fulfillment of an institution's contractual obligations to deliver funds (ultimately in the form of cash). Assets vary by structure, maturity, credit quality, marketability, and other characteristics that generally reflect their relative ability to be convertible into cash.

Cash operating accounts that include vault cash, cash items in process, correspondent accounts, accounts with the Federal Reserve, and other cash or "near-cash" instruments are the primary tools institutions use to execute their immediate cash-transaction obligations. They are generally not regarded as sources of additional or incremental liquidity but act as the operating levels of cash necessary for executing day-to-day transactions. Accordingly, well-managed institutions maintain ongoing balances in such accounts to meet daily business transactions. Because they generate no or very low interest earnings, such holdings are generally maintained at the minimum levels necessary to meet day-to-day transaction needs.

Beyond cash and near-cash instruments, the extent to which assets contribute to an institution's liquidity profile and the management of liquidity risk depends heavily on the contractual and structural features that determine an asset's cash-flow profile, its marketability, and its ability to be pledged to secure borrowings. The following sections discuss important aspects of these asset characteristics that effective managers factor into their management of liquidity risk on an ongoing basis and during adverse liquidity events.

Structural cash-flow attributes of assets. Knowledge and understanding of the contractual and structural features of assets, such as their maturity, interest and amortization payment schedules, and any options (either explicit or embedded) that might affect contractual cash flows under alternative scenarios, is critical for the adequate measurement and management of liquidity risk. Clearly, the maturity of assets is a key input in cash-flow analysis. Indeed, the management of asset maturities is a critical tool used in matching expected cash outflows and inflows. This matching is generally accomplished by "laddering" asset maturities in order to meet scheduled cash needs out through short and intermediate time horizons.

Short-term money market assets (MMAs) are the primary "laddering" tools used to meet funding gaps over short-term time horizons. They provide vehicles for institutions to ensure future cash availability while earning a return.

Exhibit 4—Example Summary Contingent-Liquidity-Exposure Report (Across Various Time Horizons)

	Projected liquidity cushion				
	1 week	2–4 weeks	2 months	3 months	4+ months
Normal course of business					
Total cash inflows	___	___	___	___	___
Total cash outflows	___	___	___	___	___
Liquidity cushion (shortfall)	___	___	___	___	___
Liquidity coverage ratio	___	___	___	___	___
Mild institution-specific					
Total cash inflows	___	___	___	___	___
Total cash outflows	___	___	___	___	___
Liquidity cushion (shortfall)	___	___	___	___	___
Liquidity coverage ratio	___	___	___	___	___
Severe institution-specific					
Total cash inflows	___	___	___	___	___
Total cash outflows	___	___	___	___	___
Liquidity cushion (shortfall)	___	___	___	___	___
Liquidity coverage ratio	___	___	___	___	___
Severe credit crunch					
Total cash inflows	___	___	___	___	___
Total cash outflows	___	___	___	___	___
Liquidity cushion (shortfall)	___	___	___	___	___
Liquidity coverage ratio	___	___	___	___	___
Capital-markets disruption					
Total cash inflows	___	___	___	___	___
Total cash outflows	___	___	___	___	___
Liquidity cushion (shortfall)	___	___	___	___	___
Liquidity coverage ratio	___	___	___	___	___
Custom scenario					
Total cash inflows	___	___	___	___	___
Total cash outflows	___	___	___	___	___
Liquidity cushion (shortfall)	___	___	___	___	___
Liquidity coverage ratio	___	___	___	___	___

Given the relatively low return on such assets, managers face important tradeoffs between earnings and the provision of liquidity in deploying such assets. In general, larger institutions employ a variety of MMAs in making such tradeoffs, while smaller community organizations face fewer potential sources of short-term investments.

The contractual and structural features, such as the maturity and payment streams of all financial assets, should be factored into both cash-flow projections and the strategies developed for filling negative funding gaps. This practice includes the assessment of embedded options in assets that can materially affect an asset's cash flow. Effective liquidity managers incorporate the expected exercise of options in projecting cash flows for the various scenarios they use in measuring liquidity risk. For example, normal "business as usual" projections may include an estimate of the expected amount of loan and security principal prepayments under prevailing market interest rates, while alternative-scenario projections may employ estimates of expected increases in prepayments (and cash

flows) arising from declining interest rates and expected declines in prepayments or "maturity extensions" resulting from rising market interest rates.

Market liquidity, or the "marketability" of assets. Marketability is the ability to convert an asset into cash through a quick "sale" and at a fair price. This ability is determined by the market in which the sale transaction is conducted. In general, investment-grade securities are more marketable than loans or other assets. Institutions generally view holdings of investment securities as a first line of defense for contingency purposes, but banks need to fully assess the marketability of these holdings. The availability and size of a bid-asked spread for an asset provides a general indication of the market liquidity of that asset. The narrower the spread, and the deeper and more liquid the market, the more likely a seller will find a willing buyer at or near the asked price. Importantly, however, the market liquidity of an asset is not a static attribute but is a function of conditions prevailing in the secondary markets for the particular asset. Bid-asked spreads, when they exist, generally vary with the volume and frequency of transactions in the particular type of assets. Larger volumes and greater frequency of transactions are generally associated with narrower bid-asked spreads. However, disruptions in the marketplace, contractions in the number of market makers, the execution of large block transactions in the asset, and other market factors may result in the widening of the bid-asked spread—and thus reduce the market liquidity of an instrument. Large transactions, in particular, can constrain the market liquidity of an asset, especially if the market for the asset is not deep.

The marketability of assets may also be constrained by the volatility of overall market prices and the underlying rates, which may cause widening bid-asked spreads on marketable assets. Some assets may be more subject to this type of market volatility than others. For example, securities that have inherent credit or interest-rate risk can become more difficult to trade during times when market participants have a low tolerance for these risks. This may be the case when market uncertainties prompt investors to shun risky securities in favor of more-stable investments, resulting in a so-called flight to quality. In a flight to quality, investors become much more willing to sacrifice yield in exchange for safety and liquidity.

In addition to reacting to prevailing market conditions, the market liquidity of an asset can be affected by other factors specific to individual investment positions. Small pieces of security issues, security issues from nonrated and obscure issuers, and other inactively traded securities may not be as liquid as other investments. While brokers and dealers buy and sell inactive securities, price quotations may not be readily available, or when they are, bid-asked spreads may be relatively wide. Bids for such securities are unlikely to be as high as the bids for similar but actively traded securities. Therefore, even though sparsely traded securities can almost always be sold, an unattractive price can make the seller unenthusiastic about selling or result in potential losses in order to raise cash through the sale of an asset.

Accounting conventions can also affect the market liquidity of assets. For example, Accounting Standards Codification (ASC) 320, "Investments—Debt and Equity Securities," (or Statement of Financial Accounting Standards No. 115 (FAS 115)) requires investment securities to be categorized as held-to-maturity (HTM), available-for-sale (AFS), or trading, significantly affects the liquidity characteristics of investment holdings. Of the three categories, securities categorized as HTM provide the least liquidity, as they cannot be sold to meet liquidity needs without potentially onerous repercussions.[7]

Securities categorized as AFS can be sold at any time to meet liquidity needs, but care must be taken to avoid large swings in earnings or triggering impairment recognition of securities with unrealized losses.

Trading account securities are generally considered the most marketable from an accounting standpoint, since selling a trading account investment has little or no income effect.

While securities are generally considered to have greater market liquidity than loans and other assets, liquidity-risk managers increasingly consider the ability to obtain cash from the sale of loans as a potential source of liquidity. Many types of bank loans can be sold, securitized, or pledged as collateral for borrowings. For example, the portions of loans that are insured or guaranteed by the U.S. government or by U.S. government–sponsored enterprises

7. HTM securities can be pledged, however, so they do still provide a potential source of liquidity. Furthermore, since the HTM-sale restriction is only an accounting standard (FAS 115)—not a market limitation—HTM securities can be sold in cases of extreme need.

are readily saleable under most market conditions. From a market liquidity perspective, the primary difference between loans and securities is that the process of turning loans into cash can be less efficient and more time-consuming. While securitizations of loan portfolios (discussed below) are more common in practice, commercial loans and portfolios of mortgages or retail loans can be, and often are, bought and sold by banking organizations. However, the due diligence and other requirements of these transactions generally take weeks or even months to complete, depending on the size and complexity of the loans being sold. Liquidity-risk managers may include selling marketable loans as a potential source of cash in their liquidity analyses, but they must be careful to realistically time the expected receipt of cash and should carefully consider past experience and market conditions at the expected time of sale. Institutions that do not have prior experience selling a loan or a mortgage portfolio often need more time to close a loan sale than does an institution that makes such transactions regularly. Additionally, in systemic liquidity or institution-specific credit-quality stress scenarios, the ability to sell loans outright may not be a realistic assumption.

Securitization can be a valuable method for converting otherwise illiquid assets into cash. Advances in the capital markets have made residential mortgage, credit card, student, home equity, automobile, and other loan types increasingly amenable to securitization. As a result, the securitization of loans has become an important funds-management tool at many depository institutions. Many institutions have business lines that originate assets specifically for securitization in the capital markets. However, while securitization can play an important role in managing liquidity, it can also increase liquidity risk—especially when excessive reliance is placed on securitization as a single source of funding.

Securitization can be regarded as an ongoing, reliable source of liquidity only for institutions that have experience in securitizing the specific type of loans under consideration. The time and effort involved in structuring loan securitizations make them difficult to use as a source of asset liquidity for institutions that have limited experience with this activity. Moreover, peculiarities involved in the structures used to securitize certain types of assets may introduce added complexity in managing an institution's cash flows. For example, the securitization of certain retail-credit receivables requires planning for the possible return of receivable balances arising from scheduled or early amortization, which may entail the funding of sizable balances at unexpected or inopportune times. Institutions using securitization as a source of funding should have adequate monitoring systems and ensure that such activities are fully incorporated into all aspects of their liquidity-risk management processes—which includes assessing the liquidity impact of securitizations under adverse scenarios. This assessment is especially important for institutions that originate assets specifically for securitization since market disruptions have the potential to impose the need for significant contingent liquidity if securitizations cannot be executed. As a result, effective liquidity managers ensure that the implications of securitization activities are fully considered in both their day-to-day liquidity management and their liquidity contingency planning.

Pledging of assets to secure borrowings. The potential to pledge securities, loans, or other assets to obtain funds is another important tool for converting assets into cash to meet funding needs. Since the market liquidity of assets is a significant concern to the lender of secured funds, assets with greater market liquidity are more easily pledged than less marketable assets. An institution that has a largely unpledged investment-securities portfolio has access to liquidity either through selling the investments outright or through pledging the investments as collateral for borrowings or public deposits. However, once pledged, assets are generally unavailable for supplying contingent liquidity through their sale. When preparing cash-flow projections, liquidity-risk managers do not classify pledged assets as ''liquid assets'' that can be sold to generate cash since the liquidity available from these assets has already been ''consumed'' by the institution. Accordingly, when computing liquidity measures, effective liquidity managers avoid double-counting unpledged securities as both a source of cash from the potential sale of the asset and as a source of new liabilities from the potential collateralization of the the same security. In more-sophisticated cash-flow projections, the tying of the pledged asset to the funding is made explicit.

Similar to the pledging of securities, many investments can be sold under an agreement to repurchase. This agreement provides the institu-

tion with temporary cash without having to sell the investment outright and avoids the potential earnings volatility and transaction costs that buying and selling securities would entail.

Use of haircuts in measuring the funds that can be raised through asset sales, securitizations, or repurchase agreements. The planned use of asset sales, asset securitizations, or collateralized borrowings to meet liquidity needs necessarily involves some estimation of the value of the asset at the future point in time when the asset is anticipated to be converted into cash. Based on changes in market factors, future asset values may be more or less than current values. As a result, liquidity managers generally apply discounts, or *haircuts,* to the current value of assets to represent a conservative estimate of the anticipated proceeds available from asset sales or securitization in the capital markets. Similarly, lenders in secured borrowings also apply haircuts to determine the amount to lend against pledged collateral as protection if the value of that collateral declines. In this case, the haircut represents, in addition to other factors, the portion of asset value that cannot be converted to cash because secured lenders wish to have a collateral-protection margin.

When computing cash-flow projections under alternative scenarios and developing plans to meet cash shortfalls, liquidity managers ensure that they incorporate haircuts in order to reflect the market liquidity of their assets. Such haircuts are applied consistent with both the relative market liquidity of the assets and the specific scenario utilized. In general, longer-term, riskier assets, as well as assets with less liquid markets, are assigned larger haircuts than are shorter-term, less risky assets. For example, within the securities portfolio, different haircuts might be assigned to short-term and long-term Treasuries, rated and unrated municipal bonds, and different types of mortgage securities (e.g., pass-throughs versus CMOs). When available and appropriate, historical price changes over specified time horizons equal to the time until anticipated liquidation or the term of a borrowing are used by liquidity-risk managers to establish such haircuts. Haircuts used by nationally recognized statistical ratings organizations (NRSROs) are a starting point for such calculations but should not be unduly relied on since institution- and scenario-specific considerations may have important implications.

Haircuts should be customized to the particular projected or planned scenario. For example, adverse scenarios that hypothesize a capital-markets disruption would be expected to use larger haircuts than those used in projections assuming normal markets. Under institution-specific, adverse scenarios, certain assets, such as loans anticipated for sale, securitization, or pledging, may merit higher haircuts than those used under normal business scenarios. Institutions should fully document the haircuts they use to estimate the marketability of their assets.

Bank-owned life insurance (BOLI) is a popular instrument offering tax benefits as well as life insurance on bank employees. Some BOLI policies are structured to provide liquidity; however, most BOLI policies only generate cash in the event of a covered person's death and impose substantial fees if redeemed. In general, BOLI should not be considered a liquid asset. If it is included as a potential source of funds in a cash-flow analysis, a severe haircut reflecting the terms of the BOLI contract and current market conditions should be applied.

Liquid assets and liquidity reserves. Sound practices for managing liquidity risk call for institutions to maintain an adequate reserve of liquid assets to meet both normal and adverse liquidity situations. Such reserves should be structured consistent with the considerations discussed above regarding the marketability of different types of assets. Many institutions identify a specific portion of their investment account to serve as a liquidity reserve, or *liquidity warehouse.* The size of liquidity reserves should be based on the institution's assessments of its liquidity-risk profile and potential liquidity needs under alternative scenarios, giving full consideration to the costs of maintaining those assets. In general, the amount of liquid assets held will be a function of the stability of the institution's funding structures and the potential for rapid loan growth. If the sources of funds are stable, if adverse-scenario cash-flow projections indicate adequate sources of contingent liquidity (including sufficient sources of unused borrowing capacity), and if asset growth is predictable, then a relatively low asset liquidity reserve may be required. The availability of the liquidity reserves should be tested from time to time. Of course, liquidity reserves should be actively managed to reflect the liquidity-risk profile of the institution and current trends that might have

a negative impact on the institution's liquidity, such as—

- trading market, national, or financial market trends that might lead rate-sensitive customers to pursue investment alternatives away from the institution;
- significant actual or planned growth in assets;
- trends evidencing a reduction in large liability accounts;
- a substantial portion of liabilities from rate-sensitive and credit-quality-sensitive customers;
- significant liability concentrations by product type or by large deposit account holders;
- a loan portfolio consisting of illiquid, nonmarketable, or unpledgeable loans;
- expectations for substantial draws on loan commitments by customers;
- significant loan concentrations by product, industry, customer, and location;
- significant portions of assets pledged against wholesale borrowings; and
- impaired access to the capital markets.

B. Liabilities

Similar to its assets, a depository institution's liabilities present a complicated array of liquidity characteristics. Banking organizations obtain funds from a wide variety of sources using an array of financial instruments. The primary characteristics that determine a liability's liquidity-risk profile include its term, optionality, and counterparty risk tolerance (which includes the counterparty's need for insurance or collateral). These features help to determine if an individual liability can be considered as stable or volatile. A stable liability is a reliable source of funds that is likely to remain available in adverse circumstances. A volatile liability is a less stable source of funds that may disappear or be unavailable to the institution under heavy price competition, deteriorating credit or market- risk conditions, and other possible adverse events. Developing assumptions on the relative stability or volatility of liabilities is a crucial step in forecasting a bank's future cash flows under various scenarios and in constructing various summary liquidity measures. As a result, effective liquidity managers segment their liabilities into volatile and stable components on the basis of the characteristics of the liability and on the risk tolerance of the counterparty. These funds may be characterized as credit-sensitive, rate-sensitive, or both.

Characteristics of stability and risk tolerance. The stability of an individual bank liability is closely related to the customer's or counterparty's risk tolerance, or its willingness and ability to lend or deposit money for a given risk and reward. Several factors affect the stability and risk tolerance of funds providers, including the fiduciary responsibilities and obligations of funds providers to their customers, the availability of insurance on the funds advanced by customers to banking organizations, the reliance of customers on public debt ratings, and the relationships funds providers have with the institution.

Institutional providers of funds to banking organizations, such as money market funds, mutual funds, trust funds, public entities, and other types of investment managers, have fiduciary obligations and responsibilities to adequately assess and monitor the relative risk-and-reward tradeoffs of the investments they make for their customers, participants, or constituencies. These fund providers are especially sensitive to receiving higher returns for higher risk, and they are more apt to withdraw funds if they sense that an institution has a deteriorating financial condition. In general, funds from sources that lend or deposit money on behalf of others are less stable than funds from sources that lend their own funds. For example, a mutual fund purchaser of an institution's negotiable CD may be expected to be less stable than a local customer buying the same CD.

Institutionally placed funds and other funds providers often depend on the published evaluations or ratings of NRSROs. Indeed, many such funds providers may have bylaws or internal guidelines that prohibit placing funds with institutions that have low ratings or, in the absence of actual guidelines, may simply be averse to retaining funds at an institution whose rating is poor or whose financial condition shows deterioration. As a result, funds provided by such investors can be highly unstable in adverse liquidity environments.

The availability of insurance on deposits or collateral on borrowed funds are also important considerations in gauging the stability of funds provided. Insured or collateralized funds are usually more stable than uninsured or unsecured funds since the funds provider ultimately relies

on a third party or the value of collateral to protect its investment.

Clearly, the nature of a customer's relationship with an institution has significant implications for the potential stability or volatility of various sources of funds. Customers who have a long-standing relationship with an institution and a variety of accounts, or who otherwise use multiple banking services at the institution, are usually more stable than other types of customers.

Finally, the sensitivity of a funds provider to the rates paid on the specific instrument or transaction used by the banking organization to access funds is also critical for the appropriate assessment of the stability or volatility of funds. Customers that are very rate-driven are more likely not to advance funds or remove existing funds from an institution if more competitive rates are available elsewhere.

All of these factors should be analyzed for the more common types of depositors and funds providers and for the instruments they use to place funds with the institution. Such assessments lead to general conclusions regarding each type of customer's or counterparty's risk sensitivity and the stability of the funds provided by the instruments they use to place funds with the institution. Exhibit 5 provides a heuristic schematic of how effective liquidity-risk managers conduct such an assessment regarding the array of their different funds providers. It uses a continuum to indicate the general level of risk sensitivity (and thus the expected stability of funds) expected for each type of depositor, customer, or investor in an institution's debt obligations. Of course, individual customers and counterparties may have various degrees of such concerns, and greater granularity is generally required in practice. An additional instrument assessment of the stability or volatility of funds raised using that instrument from each type of fund provider is a logical next step in the process of evaluating the relative stability of various sources of funds to an institution.

There are a variety of methods used to assess the relative stability of funds providers. Effective liquidity managers generally review deposit accounts by counterparty type, e.g., consumer, small business, or municipality. For each type, an effective liquidity manager evaluates the applicability of risk or stability factors, such as whether the depositor has other relationships with the institution, whether the depositor owns the funds on deposit or is acting as an agent or manager, or whether the depositor is likely to be more aware of and concerned by adverse news reports. The depositors and counterparties considered to have a significant relationship with the institution and who are less sensitive to market interest rates can be viewed as providing *stable* funding. Statistical analysis of funds volatility is often used to separate total volumes into stable and nonstable segments. While such analysis can be very helpful, it is important to be mindful that historical volatility is unlikely to include a period of acute liquidity stress.

The following discussions identify important considerations that should be factored into the assessment of the relative stability of various sources of funds utilized by banking organizations.

Maturity of liabilities used to gather funds. An important factor in assessing the stability of funds sources is the remaining contractual life of the liability. Longer-maturity liabilities obviously provide more-stable funding than do shorter maturities. Extending liability maturities to reduce liquidity risk is a common management technique and an important sound practice used by most depository institutions. It is also a major part of the cost of liquidity management, since longer-term liabilities generally require higher interest rates than are required for similar short-term liabilities.

Indeterminate maturity deposits. Evaluations of the stability of deposits with indeterminate maturities, such as various types of transaction accounts (e.g., demand deposits, negotiable order of withdrawal accounts (NOWs) or money market demand accounts (MMDAs), and savings accounts) can be made using criteria similar to those shown in exhibit 5. In doing so, effective liquidity managers recognize that the relative stability or volatility of these accounts derives from the underlying characteristics of the customers that use them and not on the account type itself. As a result, most institutions delineate the relative volatility or stability of various subgroups of these account types on the basis of customer characteristics. For example, MMDA deposits of customers who have fiduciary obligations may be less stable than those of individual retail customers. Additionally, funds acquired through a higher pricing strategy for these types of deposit accounts are generally less stable than are deposits from customers who have long-standing relationships with the institution. Increasingly, liquidity managers recog-

Exhibit 5—General Characteristics of Stable and Volatile Liabilities

	Characteristics of funds providers that affect the stability/ volatility of the funds provided				
Types of funds providers	*Fiduciary agent or own funds*	*Insured or secured*	*Reliance on public information*	*Relationship*	*Stability assessment*
Consumers	owner	yes	low	high	high
Small business	owner	in part	low	high	medium
Large corporate	owner	no	medium	medium	low
Banks	agent	no	high	medium	medium
Municipalities	agent	in part	high	medium	medium
Money market mutual funds	quasi-fiduciary	no	high	low	low
Other	—	—	—	—	—

nize that traditional measures of "core" deposits may be inappropriate, and thus these deposits require more in-depth analysis to determine their relative stability.

Assessment of the relative stability or volatility of deposits that have indeterminate maturities can be qualitative as well as quantitative, consistent with the size, complexity, and sophistication of the institution. For example, at larger institutions, models based on statistical analysis can be used to estimate the stability of various subsets of such funds under alternative liquidity environments. Such models can be used to formulate expected behaviors in reaction to rate changes and other more-typical financial events. As they do when using models to manage any type of risk, institutions should fully document and understand the assumptions and methodologies used. This is especially the case when external parties conduct such analysis. Effective liquidity managers aggressively avoid "black-box" estimates of funding behaviors.

In most cases, insured deposits from consumers may be less likely to leave the institution under many liquidity circumstances than are funds supplied by more-institutional funds providers. Absent extenuating circumstances (e.g., the deposit contract prohibits early withdrawal), funds provided by agents and fiduciaries are generally treated by banking organizations as volatile liabilities.

Certificates of deposit and time deposits. At maturity, certificates of deposit (CDs) and time deposits are subject to the general factors regarding stability and volatility discussed above, including rate sensitivity and relationship factors. Nonrelationship and highly-rate-sensitive deposits tend to be less stable than deposits placed by less-rate-sensitive customers who have close relationships with the institution. Insured CDs are generally considered more stable than uninsured "jumbo" CDs in denominations of more than $100,000. In general, jumbo CDs and negotiable CDs are more volatile sources of funds—especially during times of stress—since they may be less relationship-driven and have a higher sensitivity to potential credit problems.

Brokered deposits and other rate-sensitive deposits. Brokered deposits are funds a bank obtains, directly or indirectly, by or through any deposit broker, for deposit into one or more accounts. Thus, brokered deposits include both those in which the entire beneficial interest in a given bank deposit account or instrument is held by a single depositor and those in which the deposit broker pools funds from more than one investor for deposit in a given bank deposit account. Rates paid on brokered deposits are often higher than those paid for local-market-area retail deposits since brokered-deposit customers are generally focused on obtaining the highest FDIC-insured rate available. These rate-sensitive customers have easy access to, and are frequently well informed about, alternative markets and investments, and they may have no other relationship with or loyalty to the bank. If market conditions change or more-attractive returns become available, these customers may rapidly transfer their funds to new institutions or investments. Accordingly, these rate-sensitive depositors may exhibit characteristics more typical of wholesale investors, and liquidity-risk managers should model brokered deposits accordingly.

The use of brokered deposits is governed by

law and covered by the 2001 Joint Agency Advisory on Brokered and Rate-Sensitive Deposits.[8] Under 12 USC 1831f and 12 CFR 337.6, determination of "brokered" status is based initially on whether a bank actually obtains a deposit directly or indirectly through a deposit broker. Banks that are considered only "adequately capitalized" under the "prompt corrective action" (PCA) standard must receive a waiver from the FDIC before they can accept, renew, or roll over any brokered deposit. They are also restricted in the rates they may offer on such deposits. Banks falling below the adequately capitalized range may not accept, renew, or roll over any brokered deposit, nor solicit deposits with an effective yield more than 75 basis points above the "national rate." The national rate is defined as "a simple average of rates paid by all insured depository institutions and branches for which data are available." On a weekly basis, the "national rate" is posted on the FDIC's website. If a depository institution believes that the "national rate" does not correspond to the actual prevailing rate in the applicable market, the institution may seek a determination from the FDIC that the institution is operating in a "high-rate area." If the FDIC makes such a determination, the bank will be allowed to offer the actual prevailing rate plus 75 basis points. In any event, for deposits accepted outside the applicable market area, the bank will not be allowed to offer rates in excess of the "national rate" plus 75 basis points.

These restrictions will reduce the availability of funding alternatives as a bank's condition deteriorates. The FDIC is not authorized to grant waivers for banks that are less than adequately capitalized. Bank managers who use brokered deposits should be familiar with the regulations governing brokered deposits and understand the requirements for requesting a waiver. Further detailed information regarding brokered deposits can be found in the FDIC's Financial Institution Letter (FIL), 69-2009.

Deposits attracted over the Internet, through CD listing services, or through special advertising programs that offer premium rates to customers who do not have another banking relationship with the institution also require special monitoring. Although these deposits may not fall within the technical definition of "brokered" in 12 USC 1831f and 12 CFR 337.6, their inherent risk characteristics may be similar to those of brokered deposits. That is, such deposits are typically attractive to rate-sensitive customers who may not have significant loyalty to the bank. Extensive reliance on funding products of this type, especially those obtained from outside a bank's geographic market area, has the potential to weaken a bank's funding position in times of stress.

Under the 2001 joint agency advisory, banks are expected to perform adequate due diligence before entering any business relationship with a deposit broker; assess the potential risks to earnings and capital associated with brokered deposits; and fully incorporate the assessment and control of brokered deposits into all elements of their liquidity-risk management processes, including CFPs.

Public or government deposits. Public funds generally represent deposits of the U.S. government, state governments, and local political subdivisions; they typically require collateral to be pledged against them in the form of securities. In most banks, deposits from the U.S. government represent a much smaller portion of total public funds than that of funds obtained from states and local political subdivisions. Liquidity-risk managers generally consider the secured nature of these deposits as being a double-edged sword. On the one hand, they reduce contingent liquidity risk because secured funds providers are less credit-sensitive, and therefore their deposits may be more stable than those of unsecured funds providers. On the other hand, such deposits reduce standby liquidity by "consuming" the potential liquidity in the pledged collateral.

Rather than pledge assets as collateral for public deposits, banks may also purchase an insurance company's surety bond as coverage for public funds in excess of FDIC insurance limits. Here, the bank would not pledge assets to secure deposits, and the purchase of surety bonds would not affect the availability of funds to all depositors in the event of insolvency. The costs associated with the purchase of a surety bond must be taken into consideration when using this alternative.

Deposits from taxing authorities (most school districts and municipalities) also tend to be highly seasonal. The volume of public funds

8. Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Office of Thrift Supervision. May 11, 2001. See SR-01-14.

rises around tax due dates and falls near the end of the period before the next tax due date. This fluctuation is clearly a consideration for liquidity managers projecting cash flows for normal operations. State and local governments tend to be very rate-sensitive. Effective liquidity managers fully consider the contingent liquidity risk these deposits entail, that is, the risk that the deposits will not be maintained, renewed, or replaced unless the bank is willing to offer very competitive rates.

Eurodollar deposits. Eurodollar time deposits are certificates of deposit issued by banks outside of the United States. Large, internationally active U.S. banks may obtain Eurodollar funding through their foreign branches—including offshore branches in the Cayman Islands or other similar locales. Eurodollar deposits are usually negotiable CDs issued in amounts of $100,000 or more, with rates tied to LIBOR. Because they are negotiable, the considerations applicable to negotiable CDs set forth above also apply to Eurodollar deposits.

Federal funds purchased. Federal funds (fed funds) are excess reserves held at Federal Reserve Banks. The most common type of federal funds transaction is an overnight, unsecured loan. Transactions that are for a period longer than one day are called *term fed funds.* The day-to-day use of fed funds is a common occurrence, and fed funds are considered an important money market instrument used in managing daily liquidity needs and sources.

Many regional and money-center banks, acting in the capacity of correspondents to smaller community banks, function as both providers and purchasers of federal funds. Overnight fed funds purchased can pose a contingent liquidity risk, particularly if a bank is unable to roll over or replace the maturing borrowing under stress conditions. Term fed funds pose almost the same risk since the term is usually just a week or two. Fed funds purchased should generally be treated as a volatile source of funds.

Loans from correspondent banks. Small and medium-sized banks often negotiate loans from their principal correspondent banks. The loans are usually for short periods and may be secured or unsecured. Correspondent banks are usually moderately credit-sensitive. Accordingly, cash-flow projections for normal business conditions and mild adverse scenarios may often treat these funds as stable. However, given the credit sensitivity of such funds, projections computed for severe adverse liquidity scenarios should treat these funds as volatile.

FHLB borrowings. The Federal Home Loan Banks (FHLBs) provide loans, referred to as *advances,* to members. Advances must be secured by collateral acceptable to the FHLB, such as residential mortgage loans and mortgage-backed securities. Both short-term and long-term FHLB borrowings, with maturities ranging from overnight to 10 years, are available to member institutions at generally competitive interest rates. For some small and medium-sized banks, long-term FHLB advances may be a significant or the only source of long-term funding.

It should be noted that FHLBs may also sell their excess cash into the market in the form of fed funds. This is a transaction where the FHLB is managing its excess funding and has chosen to invest that excess in short-term unsecured fed funds. This transaction is executed through the capital markets and is not done with specific members of the FHLB.

Some FHLB advances contain embedded options or other features that may increase funding risk. For example, some types of advances, such as putable and convertible advances, provide the FHLB with the option to either recall the advance or change the interest rate on an advance from a fixed rate to a floating rate under specified conditions. When such optionality exists, institutions should fully assess the implications of this optionality on the liquidity-risk profile of the institution.

In general, an FHLB establishes a line of credit for each of its members. Members are required to purchase FHLB stock before a line of credit is established, and the FHLB has the ability to restrict the redemption of its stock. An FHLB may also limit or deny a member's request for an advance if the member engages in any unsafe or unsound practice, is inadequately capitalized, sustains operating losses, is deficient with respect to financial or managerial resources, or is otherwise deficient.

Because FHLB advances are secured by collateral, the unused FHLB borrowing capacity of a bank is a function of both its eligible, unpledged collateral and its unused line of credit with its FHLB.

FHLBs have access to bank regulatory information not available to other lenders. The com-

posite rating of an institution is a factor in the approval for obtaining an FHLB advance, as well as the level of collateral required and the continuance of line availability. Because of this access to regulatory data, an FHLB can react quickly to reduce its exposure to a troubled institution by exercising options or not rolling over unsecured lines of credit. Depending on the severity of a troubled institution's condition, an FHLB has the right to increase collateral requirements or to discontinue or withdraw (at maturity) its collateralized funding program because of concerns about the quality or reliability of the collateral or other credit-related concerns. On the one hand, this right may create liquidity problems for an institution, especially if it has large amounts of short-term FHLB funding. At the same time, because FHLB advances are fully collateralized, the various FHLBs have historically worked with regulators prior to exercising their option to fully withdraw funding from members. To this extent, FHLB borrowings are viewed by many liquidity managers as a relatively stable source of funding, barring the most severe of adverse funding situations.

Sound liquidity-risk management practices call for institutions to fully document the purpose of any FHLB-borrowing transaction. Each transaction should be analyzed on an ongoing basis to determine whether the arrangement achieves the stated purpose or whether the borrowings are a sign of liquidity deficiencies. Some banks may use their FHLB line of credit to secure public funds; however, doing so will reduce their available funds and may present problems if the FHLB reduces the institution's credit line. Additionally, the institution should periodically review its borrowing agreement with the FHLB to determine the assets collateralizing the borrowings and the potential risks presented by the agreement. In some instances, the borrowing agreement may provide for collateralization by all assets not already pledged for other purposes.

Repurchase agreements and dollar rolls. The terms *repurchase agreement*[9] (repo) and *reverse repurchase agreement* refer to transactions in which a bank acquires funds by selling securities and simultaneously agreeing to repurchase the securities after a specified time at a given price, which typically includes interest at an agreed-on rate. A transaction is considered a repo when viewed from the perspective of the supplier of the securities (the borrower) and a reverse repo or matched sale–purchase agreement when described from the point of view of the supplier of funds (the lender).

A repo commonly has a near-term maturity (overnight or a few days) with tenors rarely exceeding three months. Repos are also usually arranged in large dollar amounts. Repos may be used to temporarily finance the purchase of securities and dealer securities inventories. Banking organizations also use repos as a substitute for direct borrowings. Bank securities holdings as well as loans are often sold under repurchase agreements to generate temporary working funds. These types of agreements are often used because the rate on this type of borrowing is less than the rate on unsecured borrowings, such as federal funds purchased.

U.S. government and agency securities are the most common type of instruments sold under repurchase agreements, since they are exempt from reserve requirements. However, market participants sometimes alter various contract provisions to accommodate specific investment needs or to provide flexibility in the designation of collateral. For example, some repo contracts allow substitutions of the securities subject to the repurchase commitment. These transactions are often referred to as *dollar repurchase agreements* (dollar rolls), and the initial seller's obligation is to repurchase securities that are substantially similar, but not identical, to the securities originally sold. To qualify as a financing, these agreements require the return of "substantially similar securities" and cannot exceed 12 months from the initiation of the transaction. The dollar-roll market primarily consists of agreements that involve mortgage-backed securities.

Another common repo arrangement is called an *open repo*, which provides a flexible term to maturity. An open repo is a term agreement between a dealer and a major customer in which the customer buys securities from the dealer and may sell some of them back before the final maturity date.

Effective liquidity-risk managers ensure that they are aware of special considerations and potential risks of repurchase agreements, especially when the bank enters into large-dollar-volume transactions with institutional investors or brokers. It is a fairly common practice to adjust the collateral value of the underlying

9. See section 3010.1.

securities daily to reflect changes in market prices and to maintain the agreed-on margin. Accordingly, if the market value of the repo-ed securities declines appreciably, the borrower may be asked to provide additional collateral. Conversely, if the market value of the securities rises substantially, the lender may be required to return the excess collateral to the borrower. If the value of the underlying securities exceeds the price at which the repurchase agreement was sold, the bank could be exposed to the risk of loss if the buyer is unable to perform and return the securities. This risk would increase if the securities were physically transferred to the institution or broker with which the bank has entered into the repurchase agreement.

Because these instruments are usually very short-term transactions, institutions using them incur contingent liquidity risk. Accordingly, cash-flow projections for normal and mild scenarios usually treat these funds as stable. However, projections computed for severe scenarios generally treat these funds as volatile.

International borrowings. International borrowings may be direct or indirect. Common forms of direct international borrowings include loans and short-term call money from foreign banks, borrowings from the Export-Import Bank of the United States, and overdrawn nostro accounts (due from foreign bank demand accounts). Indirect forms of borrowing include notes and trade bills rediscounted with the central banks of various countries; notes, acceptances, import drafts, or trade bills sold with the bank's endorsement or guarantee; notes and other obligations sold subject to repurchase agreements; and acceptance pool participations. In general, these borrowings are often considered to be highly volatile, nonstable sources of funds.

Federal Reserve Bank borrowings. In 2003, the Federal Reserve Board revised Regulation A to provide for primary and secondary credit programs at the discount window.[10] (See section 4025.1.) Reserve Banks will extend primary credit at a rate above the target fed funds rate on a short-term basis (typically, overnight) to eligible depository institutions, and acceptable collateral is required to secure all obligations. Discount window borrowings can be secured with an array of collateral, including consumer and commercial loans. Eligibility for primary credit is based largely on an institution's examination rating and capital status. In general, institutions with composite CAMELS ratings of 1, 2, or 3 that are at least adequately capitalized are eligible for primary credit unless supplementary information indicates their condition is not generally sound. Other conditions exist to determine eligibility for 4- and 5-rated institutions.

An institution eligible for primary credit need not exhaust other sources of funds before coming to the discount window. However, because of the above-market price of primary credit, the Reserve Banks expect institutions to mainly use the discount window as a backup source of liquidity rather than as a routine source. Generally, Reserve Banks extend primary credit on an overnight basis with minimal administrative requirements to eligible institutions. Reserve Banks may also extend primary credit to eligible institutions for periods of up to several weeks if funding is not available from other sources. These longer extensions of credit are subject to greater administrative oversight. Reserve Banks also offer secondary credit to institutions that do not qualify for primary credit. Secondary credit is another short-term backup source of liquidity, although its availability is more limited and is generally used for emergency backup purposes. Reserve Banks extend secondary credit to assist in an institution's timely return to a reliance on traditional funding sources or in the resolution of severe financial difficulties. This program entails a higher level of Reserve Bank administration and oversight than primary credit.

Treasury Tax and Loan deposits. Treasury Tax and Loan accounts (TT&L accounts) are maintained at banks by the U.S. Treasury to facilitate payments of federal withholding taxes. Banks may select either the "remittance-option" or the "note-option" method of forwarding deposited funds to the U.S. Treasury. In the remittance option, the bank remits the TT&L account deposits to the Federal Reserve Bank the next business day after deposit, and the remittance portion is not interest-bearing. The note option permits the bank to retain the TT&L deposits. In the note option, the bank debits the TT&L remittance account for the amount of the previous day's deposit and simultaneously credits the

10. See the "Interagency Advisory on the Use of the Federal Reserve's Primary Credit Program in Effective Liquidity Management," Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Federal Deposit Insurance Corporation, and Office of Thrift Supervision, July 25, 2003, and SR-03-15. See also section 3010.1.

note-option account. Note-option accounts are interest-bearing and can grow to a substantial size.

TT&L funds are considered purchased funds, evidenced by an interest-bearing, variable-rate, open-ended, secured note callable on demand by Treasury. As per 31 CFR 203.24, the TT&L balance requires pledged collateral, usually from the bank's investment portfolio. Because they are secured, TT&L balances reduce standby liquidity from investments, and because they are callable, TT&L balances are considered to be volatile and they must be carefully monitored. However, in most banks, TT&L deposits constitute only a minor portion of total liabilities.

C. Off-Balance-Sheet Obligations

Off-balance-sheet transactions have been one of the fastest-growing areas of banking activity. While these activities may not be reflected on the balance sheet, they must be thoroughly reviewed in assessing an institution's liquidity-risk profile, as they can expose the institution to significant contingent liquidity risk. Effective liquidity-risk managers pay particular attention to potential liquidity risks in loan commitments, lines of credit, performance guarantees, and financial guarantees. Banks should estimate both the amount and the timing of potential cash flows from off-balance-sheet claims.

Effective liquidity managers ensure that they consider the correlation of draws on various types of commitments that can trend with macroeconomic conditions. For example, standby letters of credit issued in lieu of construction completion bonds are often drawn when builders cannot fulfill their contracts. Some types of credit lines, such as those used to provide working capital to businesses, are most heavily used when either the borrower's accounts receivable or inventory is accumulating faster than its collections of accounts payable or sales. Liquidity-risk managers should work with the appropriate lending managers to track such trends.

In addition, funding requirements arising from some types of commitments can be highly correlated with the counterparty's credit quality. Financial standby letters of credit (SBLOCs) are often used to back the counterparty's direct financial obligations, such as commercial paper, tax-exempt securities, or the margin requirements of securities and derivatives exchanges. At some institutions, a major portion of off-balance-sheet claims consists of SBLOCs supporting commercial paper. If the institution's customer issues commercial paper supported by an SBLOC and if the customer is unable to repay the commercial paper at maturity, the holder of the commercial paper will request that the institution perform under the SBLOC. Liquidity-risk managers should work with the appropriate lending manager to (1) monitor the credit grade or default probability of such counterparties and (2) manage the industry diversification of these commitments in order to reduce the probability that multiple counterparties will be forced to draw against the bank's commitments at the same time.

Funding under some types of commitments can also be highly correlated with changes in the institution's own financial condition or perceived credit quality. Commitments supporting various types of asset-backed securities, asset-backed commercial paper, and derivatives can be subject to such contingent liquidity risk. The securitization of assets generally requires some form of credit enhancement, which can take many forms, including SBLOCs or other types of guarantees issued by a bank. Similarly, many structures employ *special-purpose entities* (SPEs) that own the collateral securing the asset-backed paper. Bank SBLOCs or guarantees often support those SPEs. As long as the institution's credit quality remains above defined minimums, which are usually based on ratings from NRSROs, few or none of the SBLOCs will fund. However, if the institution's credit rating falls below the minimum, a significant amount or all of such commitments may fund at the same time.

Financial derivatives can also give rise to contingent liquidity risk arising from financial market disruptions and deteriorating credit quality of the banking organization. Derivatives contracts should be reviewed, and their potential for early termination should be assessed and quantified, to determine the adequacy of the institution's available liquidity. Many forms of standardized derivatives contracts allow counterparties to request collateral or to terminate contracts early if the institution experiences an adverse credit event or deterioration in its financial condition. In addition, under situations of market stress, a customer may ask for early termination of some contracts. In such circumstances, an institution that owes money

on derivatives transactions may be required to deliver collateral or settle a contract early, when the institution is encountering additional funding and liquidity pressures. Early terminations may also create additional, unintended market exposures. Management and directors should be aware of these potential liquidity risks and address them in the institution's CFP. All off-balance-sheet commitments and obligations should receive the focused attention of liquidity-risk managers throughout the liquidity-risk management process.

D. Specialized Business Activities

Institutions that engage in specialized banking activities should ensure that all elements of these activities are fully incorporated into their assessment of liquidity-risk exposure and their ongoing management of the firm's liquidity. Such activities may include mortgage servicing, trading and dealer activities, and various types of fee-income-generating businesses.

Institutions engaged in significant payment, clearing, and settlement activities face particular challenges. Institutions that are active in payment, settlement, or clearing activities should ensure that they have mechanisms for measuring, monitoring, and identifying the amount of liquidity they may need to settle obligations in normal as well as stressed environments. These institutions should fully consider the unique risks that may result from their participation in different payment-system activities and factor these risks into their liquidity contingency planning. Factors that banks should consider when developing liquidity plans related to payment activities include—

- the impact of pay-in rules of individual payment systems, which may result in short-notice payment adjustments and the need to assess peak pay-in requirements that could result from the failure of another participant;
- the potential impact of operational disruptions at a payment utility and the potential need to move activity to another venue in which settlement is gross rather than net, thereby increasing liquidity requirements to settle;
- the impact that the deteriorating credit quality of the institution may have on collateral requirements, changes in intraday lending limits, and the institution's intraday funding needs; and
- for clearing and nostro service providers, the impact of potential funding needs that could be generated by their clearing customers in addition to the bank's own needs.

IV. Summary Measures of Liquidity-Risk Exposure

Cash-flow projections constructed assuming normal and adverse conditions provide a wealth of information about the liquidity profile of an institution. However, liquidity managers, bank supervisors, rating agencies, and other interested parties use a myriad of summary measures of liquidity to identify potential liquidity risk. These measures include various types of financial ratios. Many of these measures attempt to achieve some of the same insights provided by comprehensive cash-flow scenario analyses but use significantly less data. When calculated using standard definitions and comparable data, such measures provide the ability to track trends over time and facilitate comparisons across peers. At the same time, however, many summary measures necessarily entail simplifying assumptions regarding the liquidity of assets, the relative stability or volatility of liabilities, and the ability of the institution to meet potential funding needs. Supervisors, management, and other stakeholders that use these summary measures should fully understand the effect of these assumptions and the limitations associated with summary measures.

Although general industry conventions may be used to compute various summary measures, liquidity managers should ensure that the specific measures they use for internal purposes are suitably customized for their particular institution. Importantly, effective liquidity managers recognize that no single summary measure or ratio captures all of the available sources and uses of liquidity for all situations and for all time periods. Different ratios capture different facets of liquidity and liquidity risk. Moreover, the same summary measure or ratio calculated using different assumptions can also capture different facets of liquidity. This is an especially important point since, by definition, many liquidity ratios are scenario-specific. Measures constructed using normal-course-of-business assumptions can portray liquidity profiles that are significantly different from those constructed assuming stress contingency events. Indeed,

many liquidity managers use the same summary measures and financial ratios computed under alternative scenarios and assumptions to evaluate and communicate to senior management and the board of directors the institution's liquidity-risk profile and the adequacy of its CFPs.

A. Cash-Flow Ratios

Cash-flow ratios are especially valuable summary liquidity measures. These measures summarize the information contained in detailed cash-flow projections and forecasts. They are generally constructed as the ratio of total projected cash inflows divided by total projected cash outflows for a particular time period or cash-flow-projection time bucket. The ratio for a given time bucket indicates the relative amount by which the projected sources of liquidity cover projected needs. For example, a ratio of 1.20 indicates a liquidity "surplus" equal to 20 percent of projected outflows. In general, such coverage ratios are compiled for each time bucket in the cash-flow projections used to assess both normal and adverse liquidity circumstances.

Some institutions also employ cumulative cash-flow ratios that are computed as the ratio of the cumulative sum of cash inflows to the cumulative sum of cash outflows for all time buckets up to a given time bucket. However, care should be taken to recognize that cumulative cash-flow ratios used alone and without the benefit of assessing the individual time-period exposures for each of their component time buckets may mask liquidity-risk exposures that can exist at intervals up to the cumulative time horizons chosen.

B. Other Summary Liquidity Measures

Other common summary liquidity measures employ assumptions about, and depend heavily on, the assessment and characterization of the relative marketability and liquidity of assets and the relative stability or volatility of funding needs and sources, consistent with the considerations discussed in the prior section. Liquidity managers use these other measures to review historical trends, summarize their projections of potential liquidity-risk exposures under adverse liquidity conditions, and develop strategies to address contingent liquidity events. In selecting from the myriad of available measures, effective liquidity managers focus primarily on those measures that are most related to the liquidity-management strategies pursued by the institution. For example, institutions that focus on managing asset liquidity place greater emphasis on measures that gauge such conditions, while institutions placing greater emphasis on managing liability liquidity emphasize measures that address those aspects of their liquidity-risk profile.

The following discussions briefly describe some of the more common summary measures of liquidity and liquidity risk. Some of these measures are employed by liquidity managers, rating agencies, and supervisors using definitions and calculation methods amenable to publicly available Call Report or BHC Performance Report data. Because such data require the use of assumptions on the liquidity of broad classes of assets and on the stability of various types of aggregated liabilities, liquidity managers and supervisors should take full advantage of the available granularity of internal data to customize the summary measures they are using. Incorporating internal data ensures that summary measures fit the specific liquidity profile of the institution. Such customization permits a more robust assessment of the institution's liquidity-risk profile.

In general, most common summary measures of liquidity and liquidity risk can be grouped into the following three broad categories:

1. those that portray the array of assets along a continuum of liquidity and cash-flow characteristics for normal and potentially adverse circumstances
2. those that portray the array of liabilities along a continuum of potential volatility and stability characteristics under normal and potentially adverse circumstances
3. those that assess the balance between funding needs and sources based on assumptions about both the relative liquidity of assets and the relative stability of liabilities

Relative liquidity of assets. Summary measures that address the liquidity of assets usually start with assessments of the maturity or type of assets in an effort to gauge their contributions to actual cash inflows over various time horizons. In general, they represent an attempt to summarize and characterize the expected cash inflows from assets that are estimated in more-detailed

cash-flow-projection worksheets assuming normal business conditions. Summary measures assessing the liquidity of assets include such measures as—

- short-term investments (defined as maturing within a specified time period, such as 3 months, 6 months, or 1 year) as a percent of total investments, and
- short-term assets (defined as maturing within a specified time period) as a percent of total assets.

Other measures within this category attempt to assess the expected time period over which longer-term, illiquid assets may need to be funded. These measures, which use broad asset categories and employ strong assumptions on the liquidity of these assets, include—

- loans and leases as a percent of total assets, and
- long-term assets (defined as maturing beyond a specified time period) as a percent of total assets.

To better gauge the potential for assets to be used as sources of liquidity to meet uncertain future cash needs, effective liquidity managers use additional ''liquid asset'' summary measures that are customized to take into account the ability (or inability) to convert assets into cash or borrowed funds. Such measures attempt to summarize the potential for sale, securitization, or use as collateral of different types of assets, subject to appropriate scenario-specific haircuts. Such measures also attempt to recognize the constraints on potential securitization and on those assets that have already been pledged as collateral for existing borrowings. Examples of these measures include—

- marketable securities (as determined by the assessment of cash-flow, accounting, and haircut considerations discussed in the previous section) to total securities;
- marketable securities as a percent of total assets;
- marketable assets (as determined by the assessment of cash-flow, accounting, and haircut considerations discussed in the previous section) to total assets;
- pledgable assets (e.g., unpledged securities and loans) as a percent of total assets;
- pledged securities (or pledged assets) to total pledgable securities (or pledgable assets);
- securitizable assets to total assets (sometimes computed to include some assessment of the time frame that may be involved); and
- liquid assets to total assets with the measure of liquid assets being some combination of short-term assets, marketable securities, and securitizable and pledgable assets (ensuring that any pledged assets are not double-counted).

Relative stability or volatility of liabilities as a source of funding. Summary measures used to assess the relative stability or volatility of liabilities as sources of funding often start with assessments of the maturity of liabilities and their ability to be ''rolled-over'' or renewed under both normal business and potentially adverse circumstances. These measures also represent an attempt to summarize and characterize the use of actual and potential sources of funds, which are estimated in more-detailed cash-flow-projection worksheets. In fact, proper construction of many of these summary measures requires the same analytical assessments required for cash-flow projections. Such measures attempt to gauge and array the relative sensitivity and availability of different sources of funds on the basis of the anticipated behavior of various types of transactions, business activities, funds providers, or other attributes.

Given the difficulties involved in portraying funding sources across the entire continuum of stability and volatility characteristics, along with the complexity of overlaying alternative contingent scenarios on such portrayals, some common summary measures attempt to group funding sources as falling on one side or the other of this continuum. Financial ratios that attempt to portray the extent to which an institution's funding sources are stable include—

- total deposits as a percent of total liabilities or total assets;
- insured deposits as a percent of total deposits;
- deposits with indeterminate maturities as a percent of total deposits; and
- long-term liabilities (defined as maturing beyond a specified time period) to total liabilities.

These measures necessarily employ assumptions about the stability of an institution's deposit base in an attempt to define a set of relatively stable or core funding sources. Liquidity man-

agers and examiners should take care in constructing their estimates of stable or core liabilities for use in such measures. This caution has become especially important as changes in customer sophistication and interest-rate sensitivity have altered behavioral patterns and, therefore, the stability characteristics traditionally assumed for retail and other types of deposits traditionally termed "core." As a result, examiners, liquidity managers, and other parties should use more-granular breakouts of funding sources to assess the relative stability of deposits and should not place undue reliance on standardized traditional measures of core deposits. Breakouts that use such a greater granularity include—

- various breakouts of retail deposits to total deposits based on product type (MMDA, demand deposit, savings account, etc.) and customer segmentation to total deposits or liabilities;
- breakouts of various types of institutional deposits (e.g., collateralized deposits of municipal and government entities) as a percent of deposits; and
- various breakouts of brokered deposits (by size, types of fund providers, and maturity).

At the other end of the stability/volatility continuum, some summary measures focus on identifying those sources of funding that need to be rolled over in the short term under normal business conditions and those whose rollover or usage in the future may be especially sensitive to institution-specific contingent liquidity events. These measures include—

- short-term liabilities (defined as fund sources maturing within a specified time period, such as 3 months, 6 months, or 1 year) as a percent of total liabilities;
- short-term brokered deposits as a percent of total deposits;
- insured short-term brokered deposits as a percent of total deposits;
- purchased funds (including short-term liabilities such as fed funds purchased, repos, FHLB borrowings, and other funds raised in secondary markets) as a percent of total liabilities;
- uncollateralized purchased funds as a percent of total liabilities; and
- short-term purchased funds to total purchased funds.

When computing measures to assess the availability of potential sources of funds under contingent liquidity scenarios, institutions may adjust the carrying values of their liabilities in order to develop best estimates of available funding sources. Similar to the haircuts applied when assessing marketable securities and liquid assets, such adjustments endeavor to identify more-realistic rollover rates on current and potential funding sources.

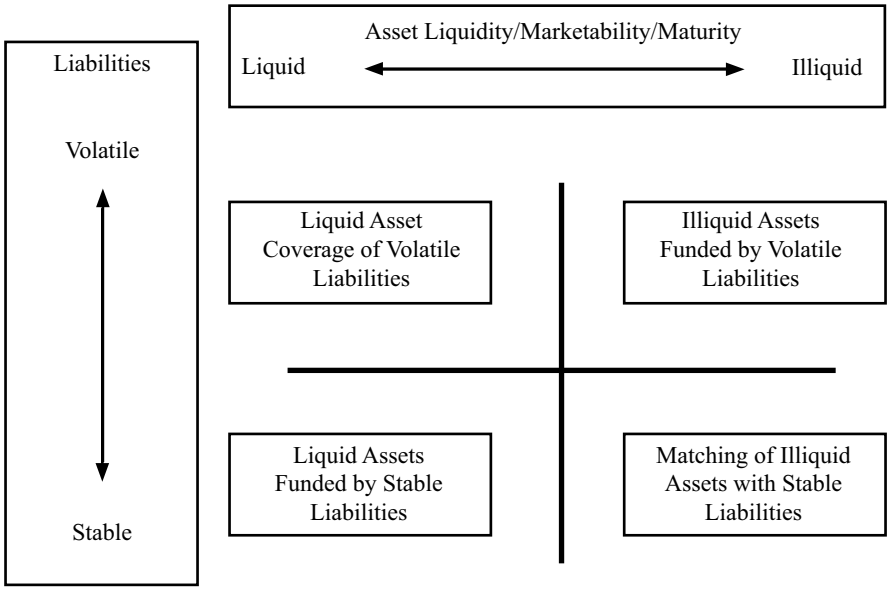
Balance between funding needs and sources. Measures used to assess the relationship between actual or potential funding needs and funding sources are constructed across a continuum that arrays both the tenor or relative liquidity of assets and the potential volatility or stability of liabilities. Many of these measures use concepts discussed earlier regarding the liquidity of assets and the relative stability or volatility of liabilities as funding sources. Some measures express various definitions of short-term liquid assets to total liabilities or alternative definitions of volatile or stable liabilities to total assets. Such measures may include—

- net short-term liabilities (short-term liabilities minus short-term assets) as a percent of total assets;
- stable deposits as a percent of total assets;
- total purchased funds as a percent of total assets;
- uncollateralized borrowings as a percent of total assets; and
- liquid assets as a percent of total liabilities.

Other measures attempt to identify the relationships between different classifications of liquid or illiquid assets and stable or volatile liabilities. Exhibit 6 provides a conceptual schematic of the range of relationships that are often addressed in such assessments.

Some commonly used summary liquidity measures and ratios focus on the amount of different types of liquid assets that are funded by various types of short-term and potentially volatile liabilities (upper-left quadrant of exhibit 6). One of the most common measures of this type is the "net short-term position" (used by some NRSROs). Liquidity managers, bank supervisors, and rating agencies use this measure to assess an institution's ability to meet its potential cash obligations over a specified period of time. It is computed as an institution's liquid assets (incorporating appropriate haircuts on

Exhibit 6—Relationships Between Liquid or Illiquid Assets and Stable or Volatile Liabilities



marketable assets) minus the potential cash obligations expected over the specified time period (e.g., 3 months, 6 months, or 1 year). Other measures used to assess the relationship or coverage of potentially volatile liabilities by liquid assets include—

- short-term investments (defined as investments maturing within a specified time period, such as 3 months, 6 months, or 1 year) as a percent of short-term and potentially volatile liabilities; and
- short-term investments (defined as investments maturing within a specified time period, such as 3 months, 6 months, or 1 year) as a percent of short-term liabilities (defined as liabilities maturing within a specified time period, such as 3 months, 6 months, or 1 year).

Other summary liquidity measures take a more expansive approach to assessing the continuum of liquid assets and volatile liabilities by including more items or expanding the breadth of analysis. Such measures include—

- liquid assets (defined as a combination of short-term assets, marketable securities, and securitizable and pledgable assets—ensuring that any pledged assets are not double-counted—over a certain specified time frame) as a percent of liabilities judged to be volatile (over the same time period);
- liquidity-surplus measures, such as liquid assets minus short-dated or volatile liabilities; and
- liquid assets as a percent of purchased funds.

Other common summary measures of liquidity focus on the potential mismatch of using short-term or potentially volatile liabilities to fund illiquid assets (upper-right-hand quadrant of exhibit 6). Often these measures factor only those volatile liabilities in excess of short-term and highly liquid assets or marketable investment securities into this assessment. Such volatile-liability-dependence measures provide insights as to the extent to which alternative funding sources might be needed to fund long-term liquidity needs under adverse liquidity conditions. These measures include—

- net short-term noncore-funding-dependence measures, such as short-term volatile funding minus short-term investments as a percent of illiquid assets; and
- net volatile-funding-dependence measures, such as volatile funding minus liquid assets as a percent of illiquid assets.

Another set of summary liquidity ratios can be constructed to focus on the extent to which illiquid assets are match-funded by stable liabilities (lower-right quadrant of exhibit 6). Common examples of such measures include traditional loan-to-deposit ratios (which incorrectly assume all deposits are stable) and loan-to-core-deposit ratios (which often take a product-specific approach to defining the stability of certain types of deposits). However, since such traditional measures necessarily require the use of broad assumptions on the stability of deposits, they should not be relied on to provide meaningful insights regarding potential funding mismatches between stable funding sources and illiquid assets.

One meaningful measure used to gauge such relationships is the concept of ''net cash capital'' (which is also used by some NRSROs). This measure is the dollar amount by which stable sources of funds exceed illiquid assets; it can be computed as a percent of total assets to facilitate comparisons across institutions. In addition, it can be computed using customized assessments of the relative stability of different types of liabilities and the ability to convert assets into cash through sale, securitization, or collateralization. For example, firms may choose to exclude portions of loans sold regularly (e.g., loans conforming to secondary-market standards) as illiquid assets, or they may choose to include long-term debt as stable liabilities.

A final set of summary measures are used by liquidity managers to optimize the liquidity profiles of their institutions. These measures assess the extent to which relatively stable funding sources are used to fund short-term and liquid assets (lower-left quadrant of exhibit 6). Since short-term liquid assets generally entail relatively lower returns than longer-term less-liquid assets, measures assessing such potential mismatches focus liquidity managers on the cost of carrying liquid assets.

V. Liquidity-Measurement Considerations for Bank Holding Companies

Liquidity-risk measurement considerations for BHCs can be found in the *Bank Holding Company Supervision Manual*, sections 4000.1, 4010, and 4020.

APPENDIX 2—SUMMARY OF MAJOR LEGAL AND REGULATORY CONSIDERATIONS

The following discussions summarize some of the major legal and regulatory considerations that should be taken into account in managing the liquidity risk of banking organizations. The discussions are presented only to highlight potential issues and to direct bankers and supervisors to source documents on those issues.

A. Federal Reserve Regulation A

Federal Reserve Regulation A addresses borrowing from the discount window. Rules defining eligible collateral can be found in this regulation.

B. Federal Reserve Regulation D

Federal Reserve Regulation D addresses required reserves for deposits. One portion of the regulation, however, restricts the type of eligible collateral that can be pledged for repurchase-agreement borrowings.

C. Federal Reserve Regulation F

Federal Reserve Regulation F imposes limits on interbank liabilities. This regulation implements section 308 of the Federal Deposit Insurance Corporation Improvement Act (FDICIA). Banks that sell funds to other banks must have written policies to limit excessive exposure, must review the financial condition or credit rating of the debtor, must have internal limits on the size of exposures that are consistent with the credit risk, may not lend more than 25 percent of their

capital to a single borrowing bank, and must undertake other steps.

Banks that borrow federal funds or other borrowings from correspondent banks may find, as a result of the seller's compliance with Regulation F, that the amount they may borrow has suddenly declined as a result of a reduction in their credit rating or credit quality. Regulation F may make it harder for a bank to use borrowings as a liquidity source for a bank-specific liquidity crisis.

D. Federal Reserve Regulation W

Federal Reserve Regulation W governs transactions between an insured bank or thrift and its affiliates. The regulation establishes a consistent and comprehensive compilation of requirements found in section 23A of the Federal Reserve Act, 70 years of Board interpretations of section 23A, section 23B of the Federal Reserve Act, and portions of the Gramm-Leach-Bliley Act of 1999. Covered transactions include purchases of assets from an affiliate, extensions of credit to an affiliate, investments in securities issued by an affiliate, guarantees on behalf of an affiliate, and certain other transactions that expose the member bank to an affiliate's credit or investment risk. Derivatives transactions and intraday extensions of credit are also covered.

The intentions of the regulation are (1) to protect the depository institution, (2) to ensure that all transactions between the bank and its affiliates are on terms and conditions that are consistent with safe and sound banking practices, and (3) to limit the ability of a depository institution to transfer to its affiliates the subsidy arising from the institution's access to the federal safety net. The regulation achieves these goals in four major ways:

1. It limits a member bank's covered transactions with any single affiliate to no more than 10 percent of the bank's capital stock and surplus, and limits transactions with all affiliates combined to no more than 20 percent of the bank's capital stock and surplus.
2. It requires all transactions between a member bank and its affiliates to be on terms and conditions that are consistent with safe and sound banking practices.
3. It prohibits a member bank from purchasing low-quality assets from its affiliates.
4. It requires that a member bank's extensions of credit to affiliates and guarantees on behalf of affiliates be appropriately secured by a statutorily defined amount of collateral.

Section 23B protects member banks by requiring that certain transactions between the bank and its affiliates occur on market terms, that is, on terms and under circumstances that are substantially the same, or at least as favorable to the bank, as those prevailing at the time for comparable transactions with unaffiliated companies. Section 23B applies the market-terms restriction to any covered transaction (as defined in section 23A) with an affiliate as well as certain other transactions, such as (1) any sale of assets by the member bank to an affiliate, (2) any payment of money or furnishing of services by the member bank to an affiliate, and (3) any transaction by the member bank with a third party if an affiliate has a financial interest in the third party or if an affiliate is a participant in the transaction.

Liquidity-risk managers working in banks that have affiliates must give careful attention to Regulation W, which addresses transactions between banks and their affiliates. In the normal course of business, the prohibition on unsecured funding can tie up collateral, complicate collateral management, and restrict the availability of funding from affiliates. In stressed conditions, all of those problems—plus the size limit and the prohibition on sales of low-quality assets to affiliates—effectively close down many transactions with affiliates.

E. Statutory Restriction of FHLB Advances

The Federal Home Loan Banks (FHLBs) provide a number of different advance programs with very attractive terms to member banks. Many banks now use the FHLBs for term funding. The FHLBs are very credit-sensitive lenders.

A federal regulation (12 CFR 935, Federal Housing Finance Board—Advances) requires the FHLBs to be credit-sensitive. In addition to monitoring the general financial condition of commercial banks and using rating information provided by bank rating agencies, the FHLBs have access to nonpublic regulatory information and supervisory actions taken

against banks. The FHLBs often react quickly, sometimes before other funds providers, to reduce exposure to a troubled bank by not rolling over unsecured borrowing lines. Depending on the severity of a troubled bank's condition, even the collateralized funding program may be discontinued or withdrawn at maturity because of concerns about the quality or reliability of the collateral or other credit-related concerns. Contractual provisions requiring increases in collateral may also be invoked. Any of these changes in FHLB-loan availability or terms can create significant liquidity problems, especially in banks that use large amounts of short-term FHLB funding.

F. Statutory Restriction on the Use of Brokered Deposits

The use of brokered deposits is restricted by 12 CFR 337.6. Well-capitalized banks may accept brokered deposits without restriction. Adequately capitalized banks must obtain a waiver from the FDIC to solicit, renew, or roll over brokered deposits. Adequately capitalized banks must also comply with restrictions on the rates that they pay for these deposits. Banks that have capital levels below adequately capitalized are prohibited from using brokered deposits. In addition to these restrictions, banking regulators have also issued detailed guidance, discussed in section H below, on the use of brokered deposits.

G. Legal Restrictions on Dividends

A number of statutory restrictions limit the amount of dividends that a bank may pay to its stockholders. As a result, a bank holding company that depends on cash from its bank subsidiaries can find this source of funds limited or closed. This risk is particularly significant for bank holding companies with nonbank subsidiaries that require funding or debt service.

H. Restrictions on Investments That Affect Liquidity-Risk Management

Interagency guidance issued in 1998 by the FFIEC, "Supervisory Policy Statement on Investment Securities and End-User Activities," contains provisions that may affect liquidity and liquidity management. (See SR-98-12.) The following points summarize some of these potential impacts, although readers should review the entire rule for more-complete information.

1. When banks specify permissible instruments for accomplishing established objectives, they must take into account the liquidity of the market for those investments and the effect that liquidity may have on achieving their objective.
2. Banks are required to consider the effects that market risk can have on the liquidity of different types of instruments under various scenarios.
3. Banks are required to clearly articulate the liquidity characteristics of the instruments they use to accomplish institutional objectives.

In addition, the policy statement specifically highlights the greater liquidity risk inherent in complex and less actively traded instruments.

APPENDIX 3—INTERAGENCY GUIDANCE ON FUNDS TRANSFER PRICING RELATED TO FUNDING AND CONTINGENT LIQUIDITY RISKS

The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) issued this guidance on funds transfer pricing (FTP) practices related to funding risk (including interest rate and liquidity components) and contingent liquidity risk at large financial institutions (hereafter referred to as "firms") to address weaknesses observed in some firms' FTP practices.[11] The guidance builds on the principles of sound liquidity risk management described in the "Interagency Policy Statement on Funding and

11. For purposes of this guidance, large financial institutions includes national banks, federal savings associations and state-chartered banks with consolidated assets of $250 billion or more, domestic bank and savings and loan holding companies with consolidated assets of $250 billion or more or foreign exposure of $10 billion or more, and foreign banking organizations with combined U.S. assets of $250 billion or more.

Liquidity Risk Management,"[12] and incorporates elements of the international statement issued by the Basel Committee on Banking Supervision titled "Principles for Sound Liquidity Risk Management and Supervision."[13]

For purposes of this guidance, FTP refers to a process performed by a firm's central management function that allocates costs and benefits associated with funding and contingent liquidity risks (FTP costs and benefits), as measured at transaction or trade inception, to a firm's business lines, products, and activities. While this guidance specifically addresses FTP practices related to funding and contingent liquidity risks, firms may incorporate other risks in their overall FTP frameworks.

FTP is an important tool for managing a firm's balance sheet structure and measuring risk-adjusted profitability. By allocating funding and contingent liquidity risks to business lines, products, and activities within a firm, FTP influences the volume and terms of new business and ongoing portfolio composition. This process helps align a firm's funding and contingent liquidity risk profile and risk appetite and complements, but does not replace, broader liquidity and interest rate risk-management programs (for example, stress testing) that a firm uses to capture certain risks (for example, basis risk). If done effectively, FTP promotes more resilient, sustainable business models. FTP is also an important tool for centralizing the management of funding and contingent liquidity risks for all exposures. Through FTP, a firm can transfer these risks to a central management function that can take advantage of natural offsets, centralized hedging activities, and a broader view of the firm.

Failure to consistently and effectively apply FTP can misalign the risk-taking incentives of individual business lines with the firm's risk appetite, resulting in a misallocation of financial resources. This misallocation can arise in new business and ongoing portfolio composition where the business metrics do not reflect risks taken, thereby undermining the business model. Examples include entering into excessive off-balance sheet commitments and on-balance sheet asset growth because of mispriced funding and contingent liquidity risks.

The 2008 financial crisis exposed weak risk-management practices for allocating liquidity costs and benefits across business lines. Several firms "acknowledged that if robust FTP practices had been in place earlier, and if the systems had charged not just for funding but for liquidity risks, they would not have carried the significant levels of illiquid assets and the significant risks that were held off-balance sheet that ultimately led to sizable losses."[14] Refer to SR-16-3.

Funds Transfer Pricing Principles

A firm should have an FTP framework to support its broader risk-management and governance processes that incorporates the general principles described in this section and is commensurate with its size, complexity, business activities, and overall risk profile. The framework should incorporate FTP costs and benefits into product pricing, business metrics, and new product approval for all material business lines, products, and activities to align risk-taking incentives with the firm's risk appetite.

Principle 1: A firm should allocate FTP costs and benefits based on funding risk and contingent liquidity risk.

A firm should have an FTP framework that allocates costs and benefits based on the following risks.

- *Funding risk,* measured as the cost or benefit (including liquidity and interest rate components) of raising funds to finance ongoing business operations, should be allocated based on the characteristics of the business lines, products, and activities that give rise to those costs or benefits (for example, higher costs allocated to assets that will be held over a longer time horizon and greater benefits allocated to stable sources of funding).

12. Refer to FRB's SR-10-6, "Interagency Policy Statement on Funding and Liquidity Risk Management"; FDIC's FIL-13-2010, "Funding and Liquidity Risk Management Interagency Guidance"; and OCC Bulletin 2010-13, "Final Policy Statement: Interagency Policy Statement on Funding and Liquidity Management."

13. The Basel Committee on Banking Supervision statement on "Principles for Sound Liquidity Risk Management and Supervision" (September 2008) is available at www.bis.org/publ/bcbs144.htm.

14. Senior Supervisors Group report on "Risk Management Lessons from the Global Financial Crisis of 2008" (October 21, 2009) is available at www.newyorkfed.org/medialibrary/media/newsevents/news/banking/2009/SSG_report.pdf.

- *Contingent liquidity risk,* measured as the cost of holding standby liquidity composed of unencumbered, highly liquid assets, should be allocated to the business lines, products, and activities that pose risk of contingent funding needs during a stress event (for example, draws on credit commitments, collateral calls, deposit run-off, and increasing haircuts on secured funding).

Principle 2: A firm should have a consistent and transparent FTP framework for identifying and allocating FTP costs and benefits on a timely basis and at a sufficiently granular level, commensurate with the firm's size, complexity, business activities, and overall risk profile.

FTP costs and benefits should be allocated based on methodologies that are set forth by a firm's FTP framework. The methodologies should be transparent, repeatable, and sufficiently granular such that they align business decisions with the firm's desired funding and contingent liquidity risk appetite. To the extent a firm applies FTP at an aggregated level to similar products and activities, the firm should include the aggregating criteria in the report on FTP.[15] Additionally, the senior management group that oversees FTP should review the basis for the FTP methodologies. The attachment to this interagency guidance describes illustrative FTP methodologies that a firm may consider when implementing its FTP framework.[16]

A firm should allocate FTP costs and benefits, as measured at transaction or trade inception, to the appropriate business line, product, or activity. If a firm retains any FTP costs or benefits in a centrally managed pool pursuant to its FTP framework, it should analyze the implications of such decisions on business line incentives and the firm's overall risk profile. The firm customarily would include its findings in the report on FTP.

The FTP framework should be implemented consistently across the firm to appropriately align risk-taking incentives. While it is possible to apply different FTP methodologies within a firm due to, among other things, legal entity type or specific jurisdictional circumstances, a firm should generally implement the FTP framework in a consistent manner across its corporate structure to reduce the likelihood of misaligned incentives. If there are implementation differences across the firm, management should analyze the implications of such differences on business line incentives and the firm's overall funding and contingent liquidity risk profile. The firm customarily would include its findings in the report on FTP.

A firm should allocate, report, and update data on FTP costs and benefits at a frequency that is appropriate for the business line, product, or activity. Allocating, reporting, and updating of data should occur more frequently for trading exposures (for example, on a daily basis). Infrequent allocation, reporting, or updating of data for trading exposures (for example, based on month-end positions) may not fully capture a firm's day-to-day funding and contingent liquidity risks. For example, a firm should monitor the age of its trading exposures, and those held longer than originally intended should be reassessed and FTP costs and benefits should be reallocated based on the modified holding period.

A firm's FTP framework should address derivative activities commensurate with the size and complexity of those activities. The FTP framework may consider the fair value of current positions, the rights of rehypothecation for collateral received, and contingent outflows that may occur during a stress event.

To avoid a misalignment of risk-taking incentives, a firm should adjust its FTP costs and benefits as appropriate based on both market-wide and idiosyncratic conditions, such as trapped liquidity, reserve requirements, regulatory requirements, illiquid currencies, and settlement or clearing costs. These idiosyncratic conditions should be contemplated in the FTP framework, and the firm customarily would include a discussion of the implications in the report on FTP.

Principle 3: A firm should have a robust governance structure for FTP, including the production of a report on FTP and oversight from a senior management group and central management function.

A firm should have a senior management group that oversees FTP, which should include a broad

15. See Principle 3 for a discussion of the report on FTP.

16. The FRB, the FDIC, and the OCC will monitor evolving FTP practices in the market and may update or add to the illustrative methodologies in the interagency guidance attachment.

range of stakeholders, such as representatives from the firm's asset-liability committee (if separate from the senior management group), the treasury function, and business line and risk management functions. This group should develop the policy underlying the FTP framework, which should identify assumptions, responsibilities, procedures, and authorities for FTP. The policy should be reviewed and updated on a regular basis or when the firm's asset-liability structure or scope of activities undergoes a material change. Further, senior management with oversight responsibility for FTP should periodically, but no less frequently than quarterly, review the report on FTP to ensure that the established FTP framework is being properly implemented.

A firm should also establish a central management function tasked with implementing the FTP framework. The central management function should have visibility over the entire firm's on- and off-balance sheet exposures. Among its responsibilities, the central management function should regularly produce and analyze a report on FTP generated from accurate and reliable management information systems. The report on FTP should be at a sufficiently granular level to enable the senior management group and central management function to effectively monitor the FTP framework (for example, at the business line, product, or activity level, as appropriate). Among other items, all material approvals, such as those related to any exception to the FTP framework, including the reason for the exception, would customarily be documented in the report on FTP. The report on FTP may be standalone or included within a broader risk-management report.

Independent risk and control functions and internal audit should provide oversight of the FTP process and assess the report on FTP, which should be reviewed as appropriate to reflect changing business and financial market conditions and to maintain the appropriate alignment of incentives. Lastly, consistent with existing supervisory guidance on model risk management,[17] models used in FTP implementation should be independently validated and regularly reviewed to ensure that the models continue to perform as expected, that all assumptions remain appropriate, and that limitations are understood and appropriately mitigated.

Principle 4: A firm should align business incentives with risk-management and strategic objectives by incorporating FTP costs and benefits into product pricing, business metrics, and new product approval.

Through its FTP framework, a firm should incorporate FTP costs and benefits into product pricing, business metrics, and new product approval for all material business lines, products, and activities (both on- and off-balance sheet). The framework, the report on FTP, and any associated management information systems should be designed to provide decision makers sufficient and timely information about FTP costs and benefits so that risk-taking incentives align with the firm's strategic objectives.

The information may be either at the transaction level or, if the transactions have homogenous funding and contingent liquidity risk characteristics, at an aggregated level. In deciding whether to allocate FTP costs and benefits at the transaction or aggregated level, firms should consider advantages and disadvantages of both approaches when developing the FTP framework. Although transaction-level FTP allocations may add complexity and involve higher implementation and maintenance costs, such allocations may provide a more accurate measure of risk-adjusted profitability. A firm assigning FTP allocations at an aggregated level should have aggregation criteria based on funding and contingent liquidity risk characteristics that are transparent.

There should be ongoing dialogue between the business lines and the central function responsible for allocating FTP costs and benefits to ensure that funding and contingent liquidity risks are being captured and are well-understood for product pricing, business metrics, and new product approval. The business lines should understand the rationale for the FTP costs and benefits, and the central function should understand the funding and contingent liquidity risks implicated by the business lines' transactions. Decisions by senior management to incentivize certain behaviors through FTP costs and benefits customarily would be documented and included in the report on FTP.

17. Refer to FRB's SR-11-7, "Guidance on Model Risk Management" and OCC Bulletin 2011-12, "Supervisory Guidance on Model Risk Management."

Conclusion

A firm should use the principles laid out in this guidance to develop, implement, and maintain an effective FTP framework. In doing so, a firm's risk-taking incentives should better align with its risk-management and strategic objectives. The framework should be adequately tailored to a firm's size, complexity, business activities, and overall risk profile.

Interagency Guidance Attachment Illustrative Funds Transfer Pricing Methodologies

March 1, 2016

The FTP methodologies described below are intended for illustrative purposes only and provide examples for addressing principles set forth in the guidance. A firm's FTP framework should be commensurate with its size, complexity, business activities, and overall risk profile. In designing its FTP framework, a firm may utilize other methodologies that are consistent with the principles set forth in the guidance. Therefore, these illustrative methodologies should not be interpreted as directives for implementing any particular FTP methodology.

Non-Trading Exposures

For non-trading exposures, a firm's FTP methodology may vary based on its business activities and specific exposures. For example, certain firms may have higher concentrations of exposures that have less predictable time horizons, such as non-maturity loans and non-maturity deposits.

Matched-Maturity Marginal Cost of Funding

Matched-maturity marginal cost of funding is a commonly used methodology for non-trading exposures. Under this methodology, FTP costs and benefits are based on a firm's market cost of funds across the term structure (for example, wholesale long-term debt curve adjusted based on the composition of the firm's alternate sources of funding such as Federal Home Loan Bank advances and customer deposits). This methodology incentivizes business lines to generate stable funding (for example, core deposits) by crediting them the benefit or premium associated with such funding. It also ensures that business lines are appropriately charged the cost of funding for the life of longer-dated assets (for example, a five-year commercial loan). Given that funding costs can change over time, the market cost of funds across the term structure should be derived from reliable and readily available data sources and be well understood by FTP users.

FTP rates should, as closely as possible, match the characteristics of the transaction or the aggregated transactions to which they are applied. In determining the appropriate point on the derived FTP curve for a transaction or pool of transactions, a firm could consider a variety of characteristics, including the holding period, cash flow, re-pricing, prepayments, and expected life of the transaction or pool. For example, for a five-year commercial loan that has a rate that resets every three months and will be held to maturity, the interest rate component of the funding risk could be based on a three-month horizon for determining the FTP cost, and the liquidity component of the funding risk could be based on a five-year horizon for determining the FTP cost. Thus, the total FTP cost for holding the five-year commercial loan would be the combination of these two components.

Contingent Liquidity Risk

A firm may calculate the FTP cost related to non-trading exposure contingent liquidity risk using models based on behavioral assumptions. For example, charges for contingent commitments could be based on their modeled likelihood of drawdown, considering customer drawdown history, credit quality, and other factors; whereas, credits applied to deposits could be based on volatility and modeled behavioral maturity. A firm should document and include all modeling analyses and assumptions in the report on FTP. If behavioral assumptions used in a firm's FTP framework do not align with behavioral assumptions used in its internal stress test for similar types of non-trading exposures, the firm should document and include in the report on FTP these inconsistencies.

Trading Exposures

For trading exposures, a firm could consider a variety of factors, including the type of funding source (for example, secured or unsecured), the market liquidity of the exposure (for example, the size of the haircut relative to the overall exposure), the holding period of the position, the prevailing market conditions, and any potential impact the chosen approach could have on firm incentives and overall risk profile. If a firm's trading activities are not material, its FTP framework may require a less complex methodology for trading exposures. The following FTP methodologies have been observed for allocating FTP costs for trading exposures.

Weighted Average Cost of Debt (WACD)

WACD is the weighted average cost of outstanding firm debt, usually expressed as a spread over an index. Some firms' practices apply this rate to the amount of an asset expected to be funded unsecured (repurchase agreement market haircuts may be used to delineate between the amount being funded secured and the amount being funded unsecured). A firm using WACD should analyze whether the methodology misaligns risk-taking incentives and document such analyses in the report on FTP.

Marginal Cost of Funding

Marginal cost of funding sets the FTP costs at the appropriate incremental borrowing rate of a firm. Some firms' practices apply a marginal secured borrowing rate to the amount of an asset expected to be funded secured and a marginal unsecured borrowing rate to the amount of an asset expected to be funded unsecured (repurchase agreement market haircuts may be used to delineate between the amount being funded secured and the amount being funded unsecured). A firm using marginal cost of funding should analyze whether the methodology misaligns risk-taking incentives, considering current market rates compared to historical rates, and document such analyses in the report on FTP.

Contingent Liquidity Risk

A firm may calculate the FTP costs related to contingent liquidity risk from trading exposures by considering the unencumbered liquid assets that are held to cover the potential for widening haircuts of trading exposures that are funded secured. If haircuts used in a firm's FTP framework do not align with haircuts used in its internal stress test for similar types of trading exposures, the firm should document and include in the report on FTP these inconsistencies. Haircuts should be updated at a frequency that is appropriate for a firm's trading activities and market conditions.

A firm may also include the FTP costs related to contingent liquidity risk from potential derivative outflows in stressed market conditions, which may be due to, for example, credit rating downgrades, additional termination rights, or market shocks and volatility.

1. To appropriately risk-focus the scope of the examination (that is, ensure that the scope is appropriate, given the institution's activities and the risks they present).
2. To assess the relative volatility or stability of the institution's liability funding sources.
3. To assess the institution's access to liquidity.
4. To assess the institution's potential liquidity needs.
5. To assess (1) the institution's exposure to mismatched risk under normal business conditions and (2) its planned strategies for addressing this risk.
6. To assess the institution's exposure to contingent liquidity risk.
7. To assess the appropriateness and integrity of the institution's corporate-governance policies for management of liquidity risk.
8. To determine whether the institution's policies, procedures, and limits are adequate, given its size, complexity, and sophistication.
9. To determine if management is adequately planning for intermediate-term and longer-term liquidity or funding needs.
10. To assess the adequacy of the institution's liquidity-risk measurement systems.
11. To assess the adequacy of the institution's liquidity-risk management information systems.
12. To assess the adequacy of the institution's contingency funding plans.
13. To assess the adequacy of the institution's internal controls for its liquidity-risk management process.
14. To determine whether the institution is complying with applicable laws and regulations.

EXAMINATION SCOPE

1. Review the following documents to identify issues that may require follow-up:
   a. prior examination findings and workpapers
   b. audit reports, and
   c. ongoing monitoring risk assessments (if available)
2. Review appropriate surveillance material, including the Uniform Bank Performance Report (UBPR), BHC Performance Report, and other reports, to identify liquidity trends and the liquidity-risk profile of the institution. This review should include assessments of the marketability of assets and the relative stability or volatility of funding sources.
3. Request and review internal reports management uses to monitor liquidity risk, including the following reports:
   a. senior management, asset/liability committee (ALCO), and for the board of directors' meetings
   b. cash-flow-projection reports
   c. contingency funding plans (CFPs)
   d. funding-concentration reports
4. Request and review organizational charts and liquidity-risk management policies and procedures.
5. Review the potential liquidity-risk exposure arising from the financial condition of the institution or other trends, such as asset growth, asset quality, earnings trends, capital adequacy, market-risk exposures (interest-rate risk (IRR) exposures for both the banking book and the trading book), business-line operational considerations, and the potential for legal and reputational risk.

On the basis of the hypothesis developed for both the institution's inherent liquidity-risk exposure and the adequacy of its liquidity management, select the steps necessary to meet examination objectives from the following procedures.

ASSESSMENT OF INHERENT LIQUIDITY RISK

1. Review the institution's deposit structure. Discuss the following issues with management: the institution's customer base, costs, and pricing strategies, as well as the stability of various types of deposits. This review should include—
   a. assumptions about deposit behaviors the institution uses in making its cash-flow projections and in conducting its IRR analyses;
   b. the competitiveness of rates paid on deposits, from both a national and local-market-area perspective;
   c. lists of large depositors, potential deposit concentrations, and large deposit maturities;
   d. the institution's use of brokered deposits and deposits from entities that may be especially sensitive to market rates and credit quality; and
   e. public fund deposits, including pledging requirements and pricing policies.
2. Review the institution's use of nondeposit liabilities. Discuss with management its strategies for employing such funds, the sensitivity of such funds to market rates, and the credit quality of the institution. This review should include—
   a. the types, costs, amounts, and concentrations of nondeposit liabilities used by the institution;
   b. the strategies underlying the use of any Federal Home Loan Bank (FHLB) advances and the specific features of those borrowings, including the existence of any options, to determine if the institution adequately understands the risk profile of these borrowings;
   c. the activities the institution funds with nondeposit liabilities;
   d. the institution's use of short-term liabilities; and
   e. compliance with the written agreements for borrowings.
3. Review the institution's holdings of marketable assets as liquidity reserves. This review should include—
   a. the quality, maturity, marketability, and

amount of unpledged investment securities;
   b. pledgable and securitizable loans and existing activities in this area; and
   c. a discussion with management on its strategies for maintaining liquid asset reserves.
4. When applicable, review the institution's access to debt markets as a source of liquidity. This review should include—
   a. the strength of current short- and longer-term debt ratings, including an assessment of the potential for "watch-listing" or downgrades;
   b. the breadth of the investor base for the company's debt;
   c. current and future issuance plans;
   d. concentrations of borrowed funds;
   e. the availability to utilize FHLB or other wholesale funds providers; and
   f. the institution's reputation in the capital markets and with major funds providers.
5. Review the institution's business activities that may have a significant impact on its liquidity needs. This review should include—
   a. the institution's ability to securitize assets and the amount of its current and anticipated securitization activities;
   b. payments- or securities-processing activities and other activities that may heighten the impact of operational risk on the liquidity of the firm;
   c. the amount and nature of trading and over-the-counter (OTC) derivative activities that may have an impact on liquidity;
   d. the extent of off-balance-sheet (OBS) loan commitments;
   e. the balance-sheet composition, including significant concentrations that may have an impact on liquidity; and
   f. operational risks associated with the institution's business activities, risks inherent in the corporate structure, or external factors that may have an impact on liquidity.
6. Review the institution's cash-flow projections.
7. Discuss with management the institution's strategies for dealing with seasonal, cyclical, and planned asset-growth funding strategies, including its assessment of alternative funding sources.
8. Review and discuss with management the institution's identification of potential contingent liquidity events and the various levels of stress those events entail. Determine if the chosen scenarios are appropriate, given the institution's business activities and funding structure.
9. Review cash-flow projections the institution has constructed for selected contingent liquidity events. Review the assumptions underlying the projections, including sources of funds to be used in a contingent liquidity event and the reports and assumptions on behavioral cash flows.
10. Review the assumptions and trends in the institution's liquidity-risk "triggers."
11. Review CFPs.
12. When appropriate, review reports on liquidity-risk triggers in the institution's securitization activities.
13. On the basis of the above procedures, determine if the institution's inherent liquidity risk is low, limited, moderate, considerable, or high.

ASSESSMENT OF THE QUALITY OF LIQUIDITY-RISK MANAGEMENT

1. Review formally adopted policies and procedures, as well as reports to the board of directors and senior management, to determine the adequacy of their oversight. This review should include whether the board and senior management—
   a. have identified lines of authority and responsibility;
   b. have articulated the institution's general liquidity strategies and its approach to liquidity risk;
   c. understand the institution's liquidity CFPs; and
   d. periodically review the institution's liquidity-risk profile.
2. Review senior management structures in order to determine their adequacy for overseeing and managing the institution's liquidity. This review should include—
   a. whether the institution has designated an ALCO or other management decision-making body;
   b. the frequency of ALCO meetings and the adequacy of the reports presented;
   c. decisions made by the ALCO and validation of follow-up on those decisions,

including ongoing assessment of open issues;
   d. the technical and managerial expertise of management and personnel involved in liquidity management; and
   e. whether the institution has clearly delineated centralized and decentralized liquidity-management responsibilities.
3. Review and discuss with management the institution's liquidity-risk policies, procedures, and limits, and determine their appropriateness, comprehensiveness, and accuracy. Policies, procedures, and limits should—
   a. identify the objectives and strategies of the institution's liquidity management and its expected and preferred reliance on various sources of funds to meet liquidity needs under alternative scenarios;
   b. delineate clear lines of responsibility and accountability over liquidity-risk management and management decision-making;
   c. be consistent with institution practices;
   d. identify the process for setting and reassessing limits, and communicate the rationale for the limit structure;
   e. specify quantitative limits and guidelines that define the acceptable level of risk for the institution, such as the use of maximum and targeted amounts of cash-flow mismatches, liquidity reserves, volatile liabilities, and funding concentrations;
   f. specify the frequency and methods used to measure, monitor, and control liquidity risk; and
   g. define the specific procedures and approvals necessary for exceptions to policies, limits, and authorizations.
4. Review and discuss with management the bank's budget projections for the appropriate planning period. Ascertain if management has adequately—
   a. planned the future direction of the bank, noting the projected growth, the source of funding for the growth, and any projected changes in its asset or liability mix;
   b. developed future plans for meeting ongoing liquidity needs; and
   c. assessed the reasonableness of its plans to achieve (1) the amounts and types of funding projected and (2) the amounts and types of asset growth projected.

   Determine if management has identified alternative sources of funds if plans are not met.
5. Review the reasonableness of bank-established parameters for the use of volatile liabilities.
6. Review liquidity-risk measurement policies, procedures, methodologies, models, assumptions, and other documentation. Discuss with management the—
   a. adequacy and comprehensiveness of cash-flow projections and supporting analysis used to manage liquidity;
   b. appropriateness of summary measures and ratios to adequately reflect the liquidity-risk profile of the institution;
   c. appropriateness of the identification of stable and volatile sources of funding;
   d. comprehensiveness of alternative contingent liquidity scenarios incorporated in the ongoing estimation of liquidity needs; and
   e. the validity and appropriateness of assumptions used in constructing liquidity-risk measures.
7. Review liquidity-risk management policies, procedures, and reports. Discuss with management the frequency and comprehensiveness of liquidity-risk reporting for the various levels of management that are responsible for monitoring and managing liquidity risk. These considerations should include the following:
   a. management's need to receive reports that—
      - determine compliance with limits and controls;
      - evaluate the results of past strategies;
      - assess the potential risks and returns of proposed strategies;
      - identify the major changes in a bank's liquidity-risk profile; and
      - consolidate holding company and bank subsidiary information.
   b. the need for the reporting system to be flexible enough to—
      - quickly collect and edit data, summarize results, and adapt to changing circumstances or issues without compromising data integrity; and
      - increase the frequency of report preparation as business conditions deteriorate.
   c. the need for reports to properly focus on monitoring liquidity and supporting

decisionmaking. These reports often help bank management to monitor—
- sources and uses of cash flows (i.e., cash flows from operating, investing, and financing activities), facilitating the evaluation of trends and structural balance-sheet changes;
- CFPs;
- projected cash-flow or maturity gaps, identifying potential future liquidity needs (reports should show projections using both contractual principal and interest runoffs and maturities (original maturity dates) and behavioral principal and interest runoffs and maturities (maturities attributable to the expected behaviors of customers));
- consolidated large funds providers, identifying customer concentrations (reports should identify and aggregate major liability instruments used by large customers across all banks in the holding company); and
- the cost of funds from all significant funding sources, enabling management to quickly compare costs.

8. Review the liquidity CFP and the minutes of ALCO meetings and board meetings. Discuss with management the adequacy of the institution's—
   a. customization of its CFP to fit its liquidity-risk profile;
   b. identification of potential stress events and the various levels of stress that can occur under those events;
   c. quantitative assessment of its short-term and intermediate-term funding needs during stress events, particularly the reasonableness of the assumptions the institution used to forecast its potential liquidity needs;
   d. comprehensiveness in forecasting cash flows under stress conditions (forecasts should incorporate OBS and payment systems and the operational implications of cash-flow forecasts);
   e. identification of potential sources of liquidity under stress events;
   f. operating policies and procedures, including the delineation of responsibilities, to be implemented in stress events, for communicating with various stakeholders;
   g. prioritization of actions for responding to stress situations;
   h. identification and use of contingent liquidity-risk triggers to monitor, on an ongoing basis, the potential for contingent liquidity events; and
   i. testing of the operational elements of the CFP.
9. Determine whether the board and senior management have established clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits. Review policies, procedures, and reports to ascertain whether the institution's—
   a. measurement system adequately captures and quantifies risk;
   b. limits are comprehensive, appropriately defined, and communicated to management in a timely manner; and
   c. risk reports are regularly and formally discussed by management and whether meeting minutes are adequately documented.
10. Determine whether internal controls and information systems are adequately tested and reviewed by ascertaining if the institution's—
    a. risk-measurement tools are accurate, independent, and reliable;
    b. testing of controls is adequate and frequent enough, given the level of risk and sophistication of risk-management decisions; and
    c. reports provide relevant information, including comments on major changes in risk profiles.
11. Determine whether the liquidity-management function is audited internally or is evaluated by the risk-management function. Determine whether the audit and/or evaluation is independent and of sufficient scope.
12. Determine whether audit findings and management responses to those findings are fully documented and tracked for adequate follow-up.
13. Determine whether line management is held accountable for unsatisfactory or ineffective follow-up.
14. Determine whether risk managers give identified material weaknesses appropriate and timely attention.
15. Assess whether actions taken by management to deal with material weaknesses have been verified and reviewed for objectivity and adequacy by senior management or the board.
16. Determine whether the board and senior

management have established adequate procedures for ensuring compliance with applicable laws and regulations.

17. Assess the institution's compliance with applicable laws and regulations as they pertain to deposit accounts.
18. Assess the institution's compliance with laws and regulations, as well as potential risk exposures arising from interbank credit exposure.
19. Assess the institution's compliance with regulations A, D, F, and W; statutory restrictions on the use of brokered deposits; and legal restrictions on dividends. Assess whether CFPs comply with these regulations and restrictions.
20. On the basis of the above procedures, determine whether the quality of the institution's liquidity-risk management is unsatisfactory, marginal, fair, satisfactory, or strong.

Review the bank's internal controls, policies, practices, and procedures for managing funding liquidity risk. The bank's system should be documented completely and concisely and should include, when appropriate, narrative descriptions, flow charts, copies of forms used, and other pertinent information.

1. Has the board of directors, consistent with its duties and responsibilities, reviewed and ratified funds-management policies, practices, and procedures that include—
   a. clear lines of authority, responsibility, and accountability for liquidity-risk management decisions?
   b. an articulated general liquidity strategy and approach to liquidity-risk management?
   c. the review and approval of policies, including liquidity contingency funding plans?
   d. the specific procedures and approvals necessary for exceptions to policies, limits, and authorizations?
   e. established procedures for ensuring compliance with applicable laws and regulations?
2. Does senior management provide adequate oversight to manage the institution's liquidity risk?
   a. Has senior management established clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits?
   b. Are clear lines of responsibility and accountability delineated over liquidity-risk management and management decisionmaking?
   c. Is there a designated asset/liability committee (ALCO) or other management decisionmaking body in which liquidity risk is appropriately discussed? Does the institution have a separate liquidity-risk management function?
   d. Is the frequency of ALCO meetings appropriate, and are the reports presented at meetings adequate?
   e. Does management regularly and formally discuss risk reports, and are meeting minutes and decisions adequately documented?
   f. Is the technical and managerial expertise of management and personnel involved in liquidity management appropriate for the institution?
   g. Are senior management's centralized and decentralized liquidity-management responsibilities clearly delineated?
3. Are the institution's policies, procedures, and limits for liquidity risk appropriate and sufficiently comprehensive to adequately control the range of liquidity risk for the level of the institution's activity?
   a. Do the policies and procedures identify the objectives and strategies of the institution's liquidity management, and do they include the institution's expected and preferred reliance on various sources of funds to meet liquidity needs under alternative scenarios?
   b. Are policies and procedures consistent with institution practices?
   c. Are the limits comprehensive and appropriately defined for the institution's level of activity? Are limit exceptions communicated to management in a timely manner?
   d. Is there a formal process for setting, reassessing, and communicating the rationale for the limit structure?
   e. Do quantitative limits and guidelines define the acceptable level of risk for the institution (i.e., maximum and targeted amounts of cash-flow mismatches, liquidity reserves, volatile liabilities, funding concentrations, etc.)?
   f. Are the frequency and methods used to measure, monitor, and control liquidity risk specified?
4. Are liquidity-risk measurement methodologies, models, assumptions, and reports, as well as other liquidity-risk management documentation, sufficiently adequate, comprehensive, and appropriate?
   a. Is liquidity-risk management involved in the financial institution's new-product discussions?
   b. Has the institution developed future growth plans and ongoing funding needs, and the sources of funding to meet those needs?
   c. Has the institution developed alternative sources of funds to be used if its future plans are not met?
   d. Does management adequately utilize comprehensive cash-flow projections and

supporting analysis in order to manage the institution's liquidity?

e. Does the institution utilize appropriate summary measures and ratios that adequately reflect its liquidity-risk profile?
f. Do the above reports provide relevant information, including comments on major changes in risk profiles?
g. Does the planning and budgeting function consider liquidity requirements?
h. Are internal management reports concerning liquidity needs and sources of funds to meet those needs prepared regularly and reviewed, as appropriate, by senior management and the board of directors?

5. Does an independent party regularly review and evaluate the components of the liquidity-risk management function?
   a. Is the liquidity-risk management function audited internally, or is it evaluated by the risk-management function? Are the audit and/or evaluation of the liquidity-risk management process and controls independent and of sufficient scope?
   b. Are audit findings and management responses to those findings fully documented and tracked for adequate follow-up?
   c. Do the internal controls and internal audit reviews ensure compliance with internal liquidity-management policies and procedures?
   d. Is line management held accountable for unsatisfactory or ineffective follow-up?
   e. Do risk managers give identified material weaknesses appropriate and timely attention? Are their actions verified and reviewed for objectivity and adequacy by senior management or the board?
6. Are internal controls and information systems adequately tested and reviewed?
   a. Are risk-measurement tools accurate, independent, and reliable?
   b. Is the frequency for the testing of controls adequate, given the level of risk and sophistication of risk-management decisions?
7. On the basis of a composite evaluation, as evidenced by answers to the foregoing questions, are the internal controls and internal audit procedures considered adequate?

LIQUIDITY-RISK MANAGEMENT USING THE FEDERAL RESERVE'S PRIMARY CREDIT PROGRAM

The Federal Reserve's primary credit program (discount window) offers depository institutions an additional source of available funds (at a rate above the target federal funds rate) for managing short-term liquidity risks.[1] Management should fully assess the potential role that the Federal Reserve's primary credit program might play in managing their institution's liquidity. The primary credit program can be a viable source of very short-term backup funds. Management may find it appropriate to incorporate the availability of the primary credit program into their institution's diversified liquidity-management policies, procedures, and contingency plans. The primary credit program has the following attributes that make the discount window a viable source of backup or contingency funding for short-term purposes:

- Primary credit provides a simpler, less-burdensome administrative process and a more accessible source of backup, short-term funding.
- Primary credit can enhance diversification in short-term funding contingency plans.
- Borrowings can be secured with an array of collateral, including consumer and commercial loans.
- Requests for primary credit advances can be made anytime during the day.[2]
- There are no restrictions on the use of short-term primary credit.

If an institution incorporates primary credit into its contingency plans, the institution should ensure that it has in place with the appropriate Reserve Bank the necessary collateral arrangements and documentation. This is particularly important when the intended collateral consists of loans or other assets that may involve significant processing or lead time for pledging to the Reserve Bank.

It is a long-established sound practice for institutions to periodically test all sources of contingency funding. Accordingly, if an institution incorporates primary credit in its contingency plans, management should occasionally test the institution's ability to borrow at the discount window. The goal of such testing is to ensure that there are no unexpected impediments or complications in the case that such contingency lines need to be used.

Institutions should ensure that any planned use of primary credit is consistent with the stated purposes and objectives of the program. Under the primary credit program, the Federal Reserve generally expects to extend funds on a very short-term basis, usually overnight. Therefore, as with any other type of short-term contingency funding, institutions should ensure that any use of primary credit facilities for short-term liquidity contingencies is accompanied by viable take-out or exit strategies to replace this funding expeditiously with other sources of funding. Institutions should factor into their contingency plans an analysis of their eligibility for primary credit under various scenarios, recognizing that if their financial condition were to deteriorate, primary credit may not be available. Under those scenarios, secondary credit may be available.

Another critical element of liquidity management is an appropriate assessment of the costs and benefits of various sources of potential liquidity. This assessment is particularly important in managing short-term and day-to-day sources and uses of funds. Given the above-market rates charged on primary credit, institutions should ensure that they adequately assess the higher costs of this form of credit relative to other available sources. Extended use of any type of relatively expensive source of funds can give rise to significant earnings implications which, in turn, may lead to supervisory concerns.

It is also important to note that the Federal Reserve's primary credit facility is only one of many tools institutions may use in managing their liquidity-risk profiles. An institution's management should ensure that the institution maintains adequate access to a diversified array of readily available and confirmed funding sources,

1. See section 3010.1 for further discussion of the Federal Reserve's credit programs that are available to qualifying institutions.
2. Advances generally are booked at the end of the business day.

including liquid assets such as high-grade investment securities and a diversified mix of wholesale and retail borrowings. (See SR-03-15.)

Supervisory and Examiner Considerations

Because primary credit can serve as a viable source of backup, short-term funds, supervisors and examiners should view the occasional use of primary credit as appropriate and unexceptional. At the same time, however, supervisors and examiners should be cognizant of the implications that too-frequent use of this source of relatively expensive funds may have for the earnings, financial condition, and overall safety and soundness of the institution. Overreliance on primary credit borrowings, or any one source of short-term contingency funds, regardless of the relative costs, may be symptomatic of deeper operational or financial difficulties. Importantly, the use of primary credit, as with the use of any potential sources of contingency funding, is a management decision that must be made in the context of safe and sound banking practices.

Banking organizations should be attentive to the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused and should address those consequences through active model risk management. The key aspects of an effective model risk-management framework are described in more detail below, including robust model development, implementation, and use; effective validation; and sound governance, policies, and controls. (See SR-11-7.)

INTRODUCTION—PART I

Banks rely heavily on quantitative analysis and models in most aspects of financial decision making.[1] They routinely use models for a broad range of activities, including underwriting credits; valuing exposures, instruments, and positions; measuring risk; managing and safeguarding client assets; determining capital and reserve adequacy; and many other activities. In recent years, banks have applied models to more complex products and with more ambitious scope, such as enterprise-wide risk measurement, while the markets in which they are used have also broadened and changed. Changes in regulation have spurred some of the recent developments, particularly the U.S. regulatory capital rules for market, credit, and operational risk based on the framework developed by the Basel Committee on Banking Supervision. Even apart from these regulatory considerations, however, banks have been increasing the use of data-driven, quantitative decision making tools for a number of years.

The expanding use of models in all aspects of banking reflects the extent to which models can improve business decisions, but models also come with costs. There is the direct cost of devoting resources to develop and implement models properly. There are also the potential indirect costs of relying on models, such as the possible adverse consequences (including financial loss) of decisions based on models that are incorrect or misused. Those consequences should be addressed by active management of model risk.

This guidance describes the key aspects of effective model risk management. Part II explains the purpose and scope of the guidance, and part III gives an overview of model risk management. Part IV discusses robust model development, implementation, and use. Part V describes the components of an effective validation framework. Part VI explains the salient features of sound governance, policies, and controls over model development, implementation, use, and validation. Part VII concludes.

PURPOSE AND SCOPE—PART II

The purpose of this section is to provide comprehensive guidance for banks on effective model risk management. Rigorous model validation plays a critical role in model risk management; however, sound development, implementation, and use of models are also vital elements. Furthermore, model risk management encompasses governance and control mechanisms such as board and senior management oversight, policies and procedures, controls and compliance, and an appropriate incentive and organizational structure.

Previous guidance and other publications issued by the Office of the Comptroller of the Currency (OCC) and the Federal Reserve on the use of models pay particular attention to model validation.[2] Based on supervisory and industry experience over the past several years, this document expands on existing guidance—most importantly by broadening the scope to include

1. Unless otherwise indicated, *banks* refers to national banks and all other institutions for which the Office of the Comptroller of the Currency is the primary supervisor, and to bank holding companies, state member banks, and all other institutions for which the Federal Reserve Board is the primary supervisor.

2. For instance, the OCC provided guidance on model risk, focusing on model validation, in OCC 2000-16 (May 30, 2000), other bulletins, and certain subject matter booklets of the *Comptroller's Handbook*. The Federal Reserve issued SR-09-01, "Application of the Market Risk Rule in Bank Holding Companies and State Member Banks," which highlights various concepts pertinent to model risk management, including standards for validation and review, model validation documentation, and back-testing. The Federal Reserve's *Trading and Capital-Markets Activities Manual* also discusses validation and model risk management. In addition, the advanced-approaches risk-based capital rules (12 CFR 3, Appendix C; 12 CFR 208, Appendix F; and 12 CFR 225, Appendix G) contain explicit validation requirements for subject banking organizations.

all aspects of model risk management. Many banks may already have in place a large portion of these practices, but all banks should ensure that internal policies and procedures are consistent with the risk-management principles and supervisory expectations contained in this guidance. Details may vary from bank to bank, as practical application of this guidance should be customized to be commensurate with a bank's risk exposures, its business activities, and the complexity and extent of its model use. For example, steps taken to apply this guidance at a community bank using relatively few models of only moderate complexity might be significantly less involved than those at a larger bank where use of models is more extensive or complex.

OVERVIEW OF MODEL RISK MANAGEMENT—PART III

For the purposes of this section, the term *model* refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. A *model* consists of three components: an information input component, which delivers assumptions and data to the model; a processing component, which transforms inputs into estimates; and a reporting component, which translates the estimates into useful business information. Models meeting this definition might be used for analyzing business strategies; informing business decisions; identifying and measuring risks; valuing exposures, instruments, or positions; conducting stress testing; assessing adequacy of capital; managing client assets; measuring compliance with internal limits; maintaining the formal control apparatus of the bank; meeting financial or regulatory reporting requirements; and issuing public disclosures. The definition of *model* also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.[3]

Models are simplified representations of real-world relationships among observed characteristics, values, and events. Simplification is inevitable, due to the inherent complexity of those relationships, but also intentional, to focus attention on particular aspects considered to be most important for a given model application. Model quality can be measured in many ways: precision, accuracy, discriminatory power, robustness, stability, and reliability, to name a few. Models are never perfect, and the appropriate metrics of quality, and the effort that should be put into improving quality, depend on the situation. For example, precision and accuracy are relevant for models that forecast future values, while discriminatory power applies to models that rank order risks. In all situations, it is important to understand a model's capabilities and limitations given its simplifications and assumptions.

The use of models invariably presents model risk, which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports. Model risk can lead to financial loss, poor business and strategic decision making, or damage to a bank's reputation. Model risk occurs primarily for two reasons:

- The model may have fundamental errors and may produce inaccurate outputs when viewed against the design objective and intended business uses. The mathematical calculation and quantification exercise underlying any model generally involves application of theory, choice of sample design and numerical routines, selection of inputs and estimation, and implementation in information systems. Errors can occur at any point from design through implementation. In addition, shortcuts, simplifications, or approximations used to manage complicated problems could compromise the integrity and reliability of outputs from those calculations. Finally, the quality of model outputs depends on the quality of input data and assumptions, and errors in inputs or incorrect assumptions will lead to inaccurate outputs.
- The model may be used incorrectly or inappropriately. Even a fundamentally sound model producing accurate outputs consistent with the design objective of the model may exhibit high model risk if it is misapplied or misused. Models by their nature are simplifications of reality, and real-world events may prove those simplifications inappropriate. This is even more of a concern if a model is used outside the environment for which it was designed. Banks may do this intentionally as they apply

3. While outside the scope of this guidance, more qualitative approaches used by banking organizations—i.e., those *not* defined as models according to this guidance—should also be subject to a rigorous control process.

existing models to new products or markets, or inadvertently as market conditions or customer behavior changes. Decision makers need to understand the limitations of a model to avoid using it in ways that are not consistent with the original intent. Limitations come in part from weaknesses in the model due to its various shortcomings, approximations, and uncertainties. Limitations are also a consequence of assumptions underlying a model that may restrict the scope to a limited set of specific circumstances and situations.

Model risk should be managed like other types of risk. Banks should identify the sources of risk and assess the magnitude. Model risk increases with greater model complexity, higher uncertainty about inputs and assumptions, broader use, and larger potential impact. Banks should consider risk from individual models and in the aggregate. Aggregate model risk is affected by interaction and dependencies among models; reliance on common assumptions, data, or methodologies; and any other factors that could adversely affect several models and their outputs at the same time. With an understanding of the source and magnitude of model risk in place, the next step is to manage it properly.

A guiding principle for managing model risk is "effective challenge" of models, that is, critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes. Effective challenge depends on a combination of incentives, competence, and influence. Incentives to provide effective challenge to models are stronger when there is greater separation of that challenge from the model development process and when challenge is supported by well-designed compensation practices and corporate culture. Competence is a key to effectiveness since technical knowledge and modeling skills are necessary to conduct appropriate analysis and critique. Finally, challenge may fail to be effective without the influence to ensure that actions are taken to address model issues. Such influence comes from a combination of explicit authority, stature within the organization, and commitment and support from higher levels of management.

Even with skilled modeling and robust validation, model risk cannot be eliminated, so other tools should be used to manage model risk effectively. Among these are establishing limits on model use, monitoring model performance, adjusting or revising models over time, and supplementing model results with other analysis and information. Informed conservatism, in either the inputs or the design of a model or through explicit adjustments to outputs, can be an effective tool, though not an excuse to avoid improving models.

As is generally the case with other risks, materiality is an important consideration in model risk management. If at some banks the use of models is less pervasive and has less impact on their financial condition, then those banks may not need as complex an approach to model risk management in order to meet supervisory expectations. However, where models and model output have a material impact on business decisions, including decisions related to risk management and capital and liquidity planning, and where model failure would have a particularly harmful impact on a bank's financial condition, a bank's model risk-management framework should be more extensive and rigorous.

Model risk management begins with robust model development, implementation, and use. Another essential element is a sound model validation process. A third element is governance, which sets an effective framework with defined roles and responsibilities for clear communication of model limitations and assumptions, as well as the authority to restrict model usage. Each of these elements is discussed in the following sections.

MODEL DEVELOPMENT, IMPLEMENTATION, AND USE—PART IV

Model risk management should include disciplined and knowledgeable development and implementation processes that are consistent with the situation and goals of the model user and with bank policy. Model development is not a straightforward or routine technical process. The experience and judgment of developers, as much as their technical knowledge, greatly influence the appropriate selection of inputs and processing components. The training and experience of developers exercising such judgment affects the extent of model risk. Moreover, the modeling exercise is often a multidisciplinary activity drawing on economics, finance, statistics, mathematics, and other fields. Models are

employed in real-world markets and events and, therefore, should be tailored for specific applications and informed by business uses. In addition, a considerable amount of subjective judgment is exercised at various stages of model development, implementation, use, and validation. It is important for decision makers to recognize that this subjectivity elevates the importance of sound and comprehensive model risk-management processes.[4]

Model Development and Implementation

An effective development process begins with a clear statement of purpose to ensure that model development is aligned with the intended use. The design, theory, and logic underlying the model should be well documented and generally supported by published research and sound industry practice. The model methodologies and processing components that implement the theory, including the mathematical specification and the numerical techniques and approximations, should be explained in detail with particular attention to merits and limitations. Developers should ensure that the components work as intended, are appropriate for the intended business purpose, and are conceptually sound and mathematically and statistically correct. Comparison with alternative theories and approaches is a fundamental component of a sound modeling process.

The data and other information used to develop a model are of critical importance; there should be rigorous assessment of data quality and relevance, and appropriate documentation. Developers should be able to demonstrate that such data and information are suitable for the model and that they are consistent with the theory behind the approach and with the chosen methodology. If data proxies are used, they should be carefully identified, justified, and documented. If data and information are not representative of the bank's portfolio or other characteristics, or if assumptions are made to adjust the data and information, these factors should be properly tracked and analyzed so that users are aware of potential limitations. This is particularly important for external data and information (from a vendor or outside party), especially as they relate to new products, instruments, or activities.

An integral part of model development is testing, in which the various components of a model and its overall functioning are evaluated to determine whether the model is performing as intended. Model testing includes checking the model's accuracy, demonstrating that the model is robust and stable, assessing potential limitations, and evaluating the model's behavior over a range of input values. It should also assess the impact of assumptions and identify situations where the model performs poorly or becomes unreliable. Testing should be applied to actual circumstances under a variety of market conditions, including scenarios that are outside the range of ordinary expectations, and should encompass the variety of products or applications for which the model is intended. Extreme values for inputs should be evaluated to identify any boundaries of model effectiveness. The impact of model results on other models that rely on those results as inputs should also be evaluated. Included in testing activities should be the purpose, design, and execution of test plans, summary results with commentary and evaluation, and detailed analysis of informative samples. Testing activities should be appropriately documented.

The nature of testing and analysis will depend on the type of model and will be judged by different criteria depending on the context. For example, the appropriate statistical tests depend on specific distributional assumptions and the purpose of the model. Furthermore, in many cases statistical tests cannot unambiguously reject false hypotheses or accept true ones based on sample information. Different tests have different strengths and weaknesses under different conditions. Any single test is rarely sufficient, so banks should apply a variety of tests to develop a sound model.

Banks should ensure that the development of the more judgmental and qualitative aspects of their models is also sound. In some cases, banks may take statistical output from a model and modify it with judgmental or qualitative adjustments as part of model development. While such practices may be appropriate, banks should ensure that any such adjustments made as part of the development process are conducted in an

4. Smaller banks that rely on vendor models may be able to satisfy the standards in this guidance without an in-house staff of technical, quantitative model developers. However, even if a bank relies on vendors for basic model development, the bank should still choose the particular models and variables that are appropriate to its size, scale, and lines of business and ensure the models are appropriate for the intended use.

appropriate and systematic manner and are well documented.

Models typically are embedded in larger information systems that manage the flow of data from various sources into the model and handle the aggregation and reporting of model outcomes. Model calculations should be properly coordinated with the capabilities and requirements of information systems. Sound model risk management depends on substantial investment in supporting systems to ensure data and reporting integrity, together with controls and testing to ensure proper implementation of models, effective systems integration, and appropriate use.

Model Use

Model use provides additional opportunity to test whether a model is functioning effectively and to assess its performance over time as conditions and model applications change. It can serve as a source of productive feedback and insights from a knowledgeable internal constituency with strong interest in having models that function well and reflect economic and business realities. Model users can provide valuable business insight during the development process. In addition, business managers affected by model outcomes may question the methods or assumptions underlying the models, particularly if the managers are significantly affected by, and do not agree with, the outcome. Such questioning can be healthy if it is constructive and causes model developers to explain and justify the assumptions and design of the models.

However, challenge from model users may be weak if the model does not materially affect their results, if the resulting changes in models are perceived to have adverse effects on the business line, or if change in general is regarded as expensive or difficult. User challenges also tend not to be comprehensive because they focus on aspects of models that have the most direct impact on the user's measured business performance or compensation, and thus may ignore other elements and applications of the models. Finally, such challenges tend to be asymmetric because users are less likely to challenge an outcome that results in an advantage for them. Indeed, users may incorrectly believe that model risk is low simply because outcomes from model-based decisions appear favorable to the institution. Thus, the nature and motivation behind model users' input should be evaluated carefully, and banks should also solicit constructive suggestions and criticism from sources independent of the line of business using the model.

Reports used for business decision making play a critical role in model risk management. Such reports should be clear and comprehensible and take into account the fact that decision makers and modelers often come from quite different backgrounds and may interpret the contents in different ways. Reports that provide a range of estimates for different input-value scenarios and assumption values can give decision makers important indications of the model's accuracy, robustness, and stability as well as information on model limitations.

An understanding of model uncertainty and inaccuracy and a demonstration that the bank is accounting for them appropriately are important outcomes of effective model development, implementation, and use. Because they are by definition imperfect representations of reality, all models have some degree of uncertainty and inaccuracy. These can sometimes be quantified, for example, by an assessment of the potential impact of factors that are unobservable or not fully incorporated in the model, or by the confidence interval around a statistical model's point estimate. Indeed, using a range of outputs, rather than a simple point estimate, can be a useful way to signal model uncertainty and avoid spurious precision. At other times, only a qualitative assessment of model uncertainty and inaccuracy is possible. In either case, it can be prudent for banks to account for model uncertainty by explicitly adjusting model inputs or calculations to produce more severe or adverse model output in the interest of conservatism. Accounting for model uncertainty can also include judgmental conservative adjustments to model output, placing less emphasis on that model's output, or ensuring that the model is only used when supplemented by other models or approaches.[5]

While conservative use of models is prudent in general, banks should be careful in applying conservatism broadly or claiming to make conservative adjustments or add-ons to address

5. To the extent that models are used to generate amounts included in public financial statements, any adjustments for model uncertainty must comply with generally accepted accounting principles.

model risk, because the impact of such conservatism in complex models may not be obvious or intuitive. Model aspects that appear conservative in one model may not be truly conservative compared with alternative methods. For example, simply picking an extreme point on a given modeled distribution may not be conservative if the distribution was misestimated or misspecified in the first place. Furthermore, initially conservative assumptions may not remain conservative over time. Therefore, banks should justify and substantiate claims that model outputs are conservative with a definition and measurement of that conservatism that is communicated to model users. In some cases, sensitivity analysis or other types of stress testing can be used to demonstrate that a model is indeed conservative. Another way in which banks may choose to be conservative is to hold an additional cushion of capital to protect against potential losses associated with model risk. However, conservatism can become an impediment to proper model development and application if it is seen as a solution that dissuades the bank from making the effort to improve the model; in addition, excessive conservatism can lead model users to discount the model outputs.

As previously explained, robust model development, implementation, and use is important to model risk management. But it is not enough for model developers and users to understand and accept the model. Because model risk is ultimately borne by the bank as a whole, the bank should objectively assess model risk and the associated costs and benefits using a sound model-validation process.

MODEL VALIDATION—PART V

Model validation is the set of processes and activities intended to verify that models are performing as expected, in line with their design objectives and business uses. Effective validation helps ensure that models are sound. It also identifies potential limitations and assumptions and assesses their possible impact. As with other aspects of effective challenge, model validation should be performed by staff with appropriate incentives, competence, and influence.

All model components, including input, processing, and reporting, should be subject to validation; this applies equally to models developed in-house and to those purchased from, or developed by, vendors or consultants. The rigor and sophistication of validation should be commensurate with the bank's overall use of models, the complexity and materiality of its models, and the size and complexity of the bank's operations.

Validation involves a degree of independence from model development and use. Generally, validation should be done by people who are not responsible for development or use and do not have a stake in whether a model is determined to be valid. Independence is not an end in itself but rather helps ensure that incentives are aligned with the goals of model validation. While independence may be supported by separation of reporting lines, it should be judged by actions and outcomes, since there may be additional ways to ensure objectivity and prevent bias. As a practical matter, some validation work may be most effectively done by model developers and users; it is essential, however, that such validation work be subject to critical review by an independent party, who should conduct additional activities to ensure proper validation. Overall, the quality of the process is judged by the manner in which models are subject to critical review. This could be determined by evaluating the extent and clarity of documentation, the issues identified by objective parties, and the actions taken by management to address model issues.

In addition to independence, banks can support appropriate incentives in validation through compensation practices and performance evaluation standards that are tied directly to the quality of model validations and the degree of critical, unbiased review. In addition, corporate culture plays a role if it establishes support for objective thinking and encourages questioning and challenging of decisions.

Staff doing validation should have the requisite knowledge, skills, and expertise. A high level of technical expertise may be needed because of the complexity of many models, both in structure and in application. These staff also should have a significant degree of familiarity with the line of business using the model and the model's intended use. A model's developer is an important source of information but cannot be relied on as an objective or sole source on which to base an assessment of model quality.

Staff conducting validation work should have explicit authority to challenge developers and users and to elevate their findings, including issues and deficiencies. The individual or unit to

whom those staff report should have sufficient influence or stature within the bank to ensure that any issues and deficiencies are appropriately addressed in a timely and substantive manner. Such influence can be reflected in reporting lines, title, rank, or designated responsibilities. Influence may be demonstrated by a pattern of actual instances in which models, or the use of models, have been appropriately changed as a result of validation.

The range and rigor of validation activities conducted prior to first use of a model should be in line with the potential risk presented by use of the model. If significant deficiencies are noted as a result of the validation process, use of the model should not be allowed or should be permitted only under very tight constraints until those issues are resolved. If the deficiencies are too severe to be addressed within the model's framework, the model should be rejected. If it is not feasible to conduct necessary validation activities prior to model use because of data paucity or other limitations, that fact should be documented and communicated in reports to users, senior management, and other relevant parties. In such cases, the uncertainty about the results that the model produces should be mitigated by other compensating controls. This is particularly applicable to new models and to the use of existing models in new applications.

Validation activities should continue on an ongoing basis after a model goes into use, to track known model limitations and to identify any new ones. Validation is an important check on model use during periods of benign economic and financial conditions, when estimates of risk and potential loss can become overly optimistic, and when the data at hand may not fully reflect more stressed conditions. Ongoing validation activities help to ensure that changes in markets, products, exposures, activities, clients, or business practices do not create new model limitations. For example, if credit risk models do not incorporate underwriting changes in a timely manner, flawed and costly business decisions could be made before deterioration in model performance becomes apparent.

Banks should conduct a periodic review—at least annually but more frequently if warranted—of each model to determine whether it is working as intended and if the existing validation activities are sufficient. Such a determination could simply affirm previous validation work, suggest updates to previous validation activities, or call for additional validation activities. Material changes to models should also be subject to validation. It is generally good practice for banks to ensure that all models undergo the full validation process, as described in the following section, at some fixed interval, including updated documentation of all activities.

Effective model validation helps reduce model risk by identifying model errors, corrective actions, and appropriate use. It also provides an assessment of the reliability of a given model, based on its underlying assumptions, theory, and methods. In this way, it provides information about the source and extent of model risk. Validation also can reveal deterioration in model performance over time and can set thresholds for acceptable levels of error, through analysis of the distribution of outcomes around expected or predicted values. If outcomes fall consistently outside this acceptable range, then the models should be redeveloped.

Key Elements of Comprehensive Validation

An effective validation framework should include three core elements:

- Evaluation of conceptual soundness, including developmental evidence
- Ongoing monitoring, including process verification and benchmarking
- Outcomes analysis, including back-testing

Evaluation of Conceptual Soundness

This first element involves assessing the quality of the model design and construction. It entails review of documentation and empirical evidence supporting the methods used and variables selected for the model. Documentation and testing should convey an understanding of model limitations and assumptions. Validation should ensure that judgment exercised in model design and construction is well informed, carefully considered, and consistent with published research and with sound industry practice. Developmental evidence should be reviewed before a model goes into use and also as part of the ongoing validation process, in particular whenever there is a material change in the model.

A sound development process will produce documented evidence in support of all model

choices, including the overall theoretical construction, key assumptions, data, and specific mathematical calculations. As part of model validation, those model aspects should be subjected to critical analysis by both evaluating the quality and extent of developmental evidence and conducting additional analysis and testing as necessary. Comparison to alternative theories and approaches should be included. Key assumptions and the choice of variables should be assessed, with analysis of their impact on model outputs and particular focus on any potential limitations. The relevance of the data used to build the model should be evaluated to ensure that it is reasonably representative of the bank's portfolio or market conditions, depending on the type of model. This is an especially important exercise when a bank uses external data or the model is used for new products or activities.

Where appropriate to the particular model, banks should employ sensitivity analysis in model development and validation to check the impact of small changes in inputs and parameter values on model outputs to make sure they fall within an expected range. Unexpectedly large changes in outputs in response to small changes in inputs can indicate an unstable model. Varying several inputs simultaneously as part of sensitivity analysis can provide evidence of unexpected interactions, particularly if the interactions are complex and not intuitively clear. Banks benefit from conducting model stress testing to check performance over a wide range of inputs and parameter values, including extreme values, to verify that the model is robust. Such testing helps establish the boundaries of model performance by identifying the acceptable range of inputs as well as conditions under which the model may become unstable or inaccurate.

Management should have a clear plan for using the results of sensitivity analysis and other quantitative testing. If testing indicates that the model may be inaccurate or unstable in some circumstances, management should consider modifying certain model properties, putting less reliance on its outputs, placing limits on model use, or developing a new approach.

Qualitative information and judgment used in model development should be evaluated, including the logic, judgment, and types of information used, to establish the conceptual soundness of the model and set appropriate conditions for its use. The validation process should ensure that qualitative, judgmental assessments are conducted in an appropriate and systematic manner, are well supported, and are documented.

Ongoing Monitoring

The second core element of the validation process is ongoing monitoring. Such monitoring confirms that the model is appropriately implemented and is being used and is performing as intended.

Ongoing monitoring is essential to evaluate whether changes in products, exposures, activities, clients, or market conditions necessitate adjustment, redevelopment, or replacement of the model and to verify that any extension of the model beyond its original scope is valid. Any model limitations identified in the development stage should be regularly assessed over time, as part of ongoing monitoring. Monitoring begins when a model is first implemented in production systems for actual business use. This monitoring should continue periodically over time, with a frequency appropriate to the nature of the model, the availability of new data or modeling approaches, and the magnitude of the risk involved. Banks should design a program of ongoing testing and evaluation of model performance along with procedures for responding to any problems that appear. This program should include process verification and benchmarking.

Process verification checks that all model components are functioning as designed. It includes verifying that internal and external data inputs continue to be accurate, complete, consistent with model purpose and design, and of the highest quality available. Computer code implementing the model should be subject to rigorous quality and change control procedures to ensure that the code is correct, that it cannot be altered except by approved parties, and that all changes are logged and can be audited. System integration can be a challenge and deserves special attention because the model processing component often draws from various sources of data, processes large amounts of data, and then feeds into multiple data repositories and reporting systems. User-developed applications, such as spreadsheets or ad hoc database applications used to generate quantitative estimates, are particularly prone to model risk. As the content or composition of information changes over time, systems may need to be updated to reflect any changes in the data or its use. Reports derived from model outputs should

be reviewed as part of validation to verify that they are accurate, complete, and informative, and that they contain appropriate indicators of model performance and limitations.

Many of the tests employed as part of model development should be included in ongoing monitoring and be conducted on a regular basis to incorporate additional information as it becomes available. New empirical evidence or theoretical research may suggest the need to modify or even replace original methods. Analysis of the integrity and applicability of internal and external information sources, including information provided by third-party vendors, should be performed regularly.

Sensitivity analysis and other checks for robustness and stability should likewise be repeated periodically. They can be as useful during ongoing monitoring as they are during model development. If models only work well for certain ranges of input values, market conditions, or other factors, they should be monitored to identify situations where these constraints are approached or exceeded.

Ongoing monitoring should include the analysis of overrides with appropriate documentation. In the use of virtually any model, there will be cases where model output is ignored, altered, or reversed based on the expert judgment of model users. Such overrides are an indication that, in some respect, the model is not performing as intended or has limitations. Banks should evaluate the reasons for overrides and track and analyze override performance. If the rate of overrides is high, or if the override process consistently improves model performance, it is often a sign that the underlying model needs revision or redevelopment.

Benchmarking is the comparison of a given model's inputs and outputs to estimates from alternative internal or external data or models. It can be incorporated in model development as well as in ongoing monitoring. For credit-risk models, examples of benchmarks include models from vendor firms or industry consortia and data from retail credit bureaus. Pricing models for securities and derivatives often can be compared with alternative models that are more accurate or comprehensive but also too time-consuming to run on a daily basis. Whatever the source, benchmark models should be rigorous, and benchmark data should be accurate and complete to ensure a reasonable comparison.

Discrepancies between the model output and benchmarks should trigger investigation into the sources and degree of the differences, and examination of whether they are within an expected or appropriate range given the nature of the comparison. The results of that analysis may suggest revisions to the model. However, differences do not necessarily indicate that the model is in error. The benchmark itself is an alternative prediction, and the differences may be due to the different data or methods used. If the model and the benchmark match well, that is evidence in favor of the model, but it should be interpreted with caution so the bank does not get a false degree of comfort.

Outcomes Analysis

The third core element of the validation process is outcomes analysis, a comparison of model outputs to corresponding actual outcomes. The precise nature of the comparison depends on the objectives of a model and might include an assessment of the accuracy of estimates or forecasts, an evaluation of rank-ordering ability, or other appropriate tests. In all cases, such comparisons help to evaluate model performance by establishing expected ranges for those actual outcomes in relation to the intended objectives and assessing the reasons for observed variation between the two. If outcomes analysis produces evidence of poor performance, the bank should take action to address those issues. Outcomes analysis typically relies on statistical tests or other quantitative measures. It can also include expert judgment to check the intuition behind the outcomes and confirm that the results make sense. When a model itself relies on expert judgment, quantitative outcomes analysis helps to evaluate the quality of that judgment. Outcomes analysis should be conducted on an ongoing basis to test whether the model continues to perform in line with design objectives and business uses.

A variety of quantitative and qualitative testing and analytical techniques can be used in outcomes analysis. The choice of technique should be based on the model's methodology, and its complexity, data availability, and the magnitude of potential model risk to the bank. Outcomes analysis should involve a range of tests because any individual test will have weaknesses. For example, some tests are better at checking a model's ability to rank-order or segment observations on a relative basis, whereas others are better at checking absolute forecast

accuracy. Tests should be designed for each situation, as not all will be effective or feasible in every circumstance, and attention should be paid to choosing the appropriate type of outcomes analysis for a particular model.

Models are regularly adjusted to take into account new data or techniques, or because of deterioration in performance. Parallel outcomes analysis, under which both the original and adjusted models' forecasts are tested against realized outcomes, provides an important test of such model adjustments. If the adjusted model does not outperform the original model, developers, users, and reviewers should realize that additional changes—or even a wholesale redesign—are likely necessary before the adjusted model replaces the original one.

Back-testing is one form of outcomes analysis; specifically, it involves the comparison of actual outcomes with model forecasts during a sample time period not used in model development and at an observation frequency that matches the forecast horizon or performance window of the model. The comparison is generally done using expected ranges or statistical confidence intervals around the model forecasts. When outcomes fall outside those intervals, the bank should analyze the discrepancies and investigate the causes that are significant in terms of magnitude or frequency. The objective of the analysis is to determine whether differences stem from the omission of material factors from the model, whether they arise from errors with regard to other aspects of model specification such as interaction terms or assumptions of linearity, or whether they are purely random and thus consistent with acceptable model performance. Analysis of in-sample fit and of model performance in holdout samples (data set aside and not used to estimate the original model) are important parts of model development but are not substitutes for back-testing.

A well-known example of back-testing is the evaluation of value-at-risk (VaR), in which actual profit and loss is compared with a model forecast loss distribution. Significant deviation in expected versus actual performance and unexplained volatility in the profits and losses of trading activities may indicate that hedging and pricing relationships are not adequately measured by a given approach. Along with measuring the frequency of losses in excess of a single VaR percentile estimator, banks should use other tests, such as assessing any clustering of exceptions and checking the distribution of losses against other estimated percentiles.

Analysis of the results of even high-quality and well-designed back-testing can pose challenges, since it is not a straightforward, mechanical process that always produces unambiguous results. The purpose is to test the model, not individual forecast values. Back-testing may entail analysis of a large number of forecasts over different conditions at a point in time or over multiple time periods. Statistical testing is essential in such cases, yet such testing can pose challenges in both the choice of appropriate tests and the interpretation of results; banks should support and document both the choice of tests and the interpretation of results.

Models with long forecast horizons should be back-tested, but given the amount of time it would take to accumulate the necessary data, that testing should be supplemented by evaluation over shorter periods. Banks should employ outcomes analysis consisting of "early warning" metrics designed to measure performance beginning very shortly after model introduction and trend analysis of performance over time. These outcomes analysis tools are not substitutes for back-testing, which should still be performed over the longer time period, but rather are very important complements.

Outcomes analysis and the other elements of the validation process may reveal significant errors or inaccuracies in model development or outcomes that consistently fall outside the bank's predetermined thresholds of acceptability. In such cases, model adjustment, recalibration, or redevelopment is warranted. Adjustments and recalibration should be governed by the principle of conservatism and should undergo independent review.

Material changes in model structure or technique, and all model redevelopment, should be subject to validation activities of appropriate range and rigor before implementation. At times, banks may have a limited ability to use key model validation tools like back-testing or sensitivity analysis for various reasons, such as lack of data or of price observability. In those cases, even more attention should be paid to the model's limitations when considering the appropriateness of model usage, and senior management should be fully informed of those limitations when using the models for decision making. Such scrutiny should be applied to individual models and models in the aggregate.

Validation of Vendor and Other Third-Party Products

The widespread use of vendor and other third-party products—including data, parameter values, and complete models—poses unique challenges for validation and other model risk-management activities because the modeling expertise is external to the user and because some components are considered proprietary. Vendor products should nevertheless be incorporated into a bank's broader model risk-management framework, following the same principles as applied to in-house models, although the process may be somewhat modified.

As a first step, banks should ensure that there are appropriate processes in place for selecting vendor models. Banks should require the vendor to provide developmental evidence explaining the product components, design, and intended use, to determine whether the model is appropriate for the bank's products, exposures, and risks. Vendors should provide appropriate testing results that show their product works as expected. They should also clearly indicate the model's limitations and assumptions and where the product's use may be problematic. Banks should expect vendors to conduct ongoing performance monitoring and outcomes analysis, with disclosure to their clients, and to make appropriate modifications and updates over time.

Banks are expected to validate their own use of vendor products. External models may not allow full access to computer coding and implementation details, so the bank may have to rely more on sensitivity analysis and benchmarking. Vendor models are often designed to provide a range of capabilities and so may need to be customized by a bank for its particular circumstances. A bank's customization choices should be documented and justified as part of validation. If vendors provide input data or assumptions, or use them to build models, their relevance for the bank's situation should be investigated. Banks should obtain information regarding the data used to develop the model and assess the extent to which that data are representative of the bank's situation. The bank also should conduct ongoing monitoring and outcomes analysis of vendor model performance using the bank's own outcomes.

Systematic procedures for validation help the bank to understand the vendor product and its capabilities, applicability, and limitations. Such detailed knowledge is necessary for basic controls of bank operations. It is also very important for the bank to have as much knowledge in-house as possible, in case the vendor or the bank terminates the contract for any reason, or if the vendor is no longer in business. Banks should have contingency plans for instances when the vendor model is no longer available or cannot be supported by the vendor.

GOVERNANCE, POLICIES, AND CONTROLS—PART VI

Developing and maintaining strong governance, policies, and controls over the model risk-management framework is fundamentally important to its effectiveness. Even if model development, implementation, use, and validation are satisfactory, a weak governance function will reduce the effectiveness of overall model risk management. A strong governance framework provides explicit support and structure to risk-management functions through policies defining relevant risk-management activities, procedures that implement those policies, allocation of resources, and mechanisms for evaluating whether policies and procedures are being carried out as specified. Notably, the extent and sophistication of a bank's governance function is expected to align with the extent and sophistication of model usage.

Board of Directors and Senior Management

Model risk governance is provided at the highest level by the board of directors and senior management when they establish a bank-wide approach to model risk management. As part of their overall responsibilities, a bank's board and senior management should establish a strong model risk-management framework that fits into the broader risk management of the organization. That framework should be grounded in an understanding of model risk—not just for individual models but also in the aggregate. The framework should include standards for model development, implementation, use, and validation.

While the board is ultimately responsible, it generally delegates to senior management the responsibility for executing and maintaining an

effective model risk-management framework. Duties of senior management include establishing adequate policies and procedures and ensuring compliance, assigning competent staff, overseeing model development and implementation, evaluating model results, ensuring effective challenge, reviewing validation and internal audit findings, and taking prompt remedial action when necessary. In the same manner as for other major areas of risk, senior management, directly and through relevant committees, is responsible for regularly reporting to the board on significant model risk, from individual models and in the aggregate, and on compliance with policy. Board members should ensure that the level of model risk is within their tolerance and should direct changes where appropriate. These actions will set the tone for the whole organization about the importance of model risk and the need for active model risk management.

Policies and Procedures

Consistent with good business practices and existing supervisory expectations, banks should formalize model risk-management activities with policies and the procedures to implement them. Model risk-management policies should be consistent with this guidance and also be commensurate with the bank's relative complexity, business activities, corporate culture, and overall organizational structure. The board or its delegates should approve model risk-management policies and review them annually to ensure consistent and rigorous practices across the organization. Those policies should be updated as necessary to ensure that model risk-management practices remain appropriate and keep current with changes in market conditions, bank products and strategies, bank exposures and activities, and practices in the industry. All aspects of model risk management should be covered by suitable policies, including model and model risk definitions; assessment of model risk; acceptable practices for model development, implementation, and use; appropriate model validation activities; and governance and controls over the model risk-management process.

Policies should emphasize testing and analysis and promote the development of targets for model accuracy, standards for acceptable levels of discrepancies, and procedures for review of, and response to, unacceptable discrepancies. They should include a description of the processes used to select and retain vendor models, including the people who should be involved in such decisions.

The prioritization, scope, and frequency of validation activities should be addressed in these policies. They should establish standards for the extent of validation that should be performed before models are put into production and the scope of ongoing validation. The policies should also detail the requirements for validation of vendor models and third-party products. Finally, they should require maintenance of detailed documentation of all aspects of the model risk-management framework, including an inventory of models in use, results of the modeling and validation processes, and model issues and their resolution.

Policies should identify the roles and assign responsibilities within the model risk-management framework with clear detail on staff expertise, authority, reporting lines, and continuity. They should also outline controls on the use of external resources for validation and compliance and specify how that work will be integrated into the model risk-management framework.

Roles and Responsibilities

Conceptually, the roles in model risk management can be divided among ownership, controls, and compliance. While there are several ways in which banks can assign the responsibilities associated with these roles, it is important that reporting lines and incentives be clear, with potential conflicts of interest identified and addressed.

Business units are generally responsible for the model risk associated with their business strategies. The role of model owner involves ultimate accountability for model use and performance within the framework set by bank policies and procedures. Model owners should be responsible for ensuring that models are properly developed, implemented, and used. The model owner should also ensure that models in use have undergone appropriate validation and approval processes, promptly identify new or changed models, and provide all necessary information for validation activities.

Model risk taken by business units should be controlled. The responsibilities for risk controls

may be assigned to individuals, committees, or a combination of the two, and include risk measurement, limits, and monitoring. Other responsibilities include managing the independent validation and review process to ensure that effective challenge takes place. Appropriate resources should be assigned for model validation and for guiding the scope and prioritization of work. Issues and problems identified through validation and other forms of oversight should be communicated by risk-control staff to relevant individuals and business users throughout the organization, including senior management, with a plan for corrective action. Control staff should have the authority to restrict the use of models and monitor any limits on model usage. While they may grant exceptions to typical procedures of model validation on a temporary basis, that authority should be subject to other control mechanisms, such as timelines for completing validation work and limits on model use.

Compliance with policies is an obligation of model owners and risk-control staff, and there should be specific processes in place to ensure that these roles are being carried out effectively and in line with policy. Documentation and tracking of activities surrounding model development, implementation, use, and validation are needed to provide a record that makes compliance with policy transparent.

Internal Audit

A bank's internal audit function should assess the overall effectiveness of the model risk-management framework, including the framework's ability to address both types of model risk for individual models and in the aggregate. Findings from internal audit related to models should be documented and reported to the board or its appropriately delegated agent. Banks should ensure that internal audit operates with the proper incentives, has appropriate skills, and has adequate stature in the organization to assist in model risk management. Internal audit's role is not to duplicate model risk-management activities. Instead, its role is to evaluate whether model risk management is comprehensive, rigorous, and effective. To accomplish this evaluation, internal audit staff should possess sufficient expertise in relevant modeling concepts as well as their use in particular business lines. If some internal audit staff perform certain validation activities, then they should not be involved in the assessment of the overall model risk-management framework.

Internal audit should verify that acceptable policies are in place and that model owners and control groups comply with those policies. Internal audit should also verify records of model use and validation to test whether validations are performed in a timely manner and whether models are subject to controls that appropriately account for any weaknesses in validation activities. Accuracy and completeness of the model inventory should be assessed. In addition, processes for establishing and monitoring limits on model usage should be evaluated. Internal audit should determine whether procedures for updating models are clearly documented and test whether those procedures are being carried out as specified. Internal audit should check that model owners and control groups are meeting documentation standards, including risk reporting. Additionally, internal audit should perform assessments of supporting operational systems and evaluate the reliability of data used by models.

Internal audit also has an important role in ensuring that validation work is conducted properly and that appropriate effective challenge is being carried out. It should evaluate the objectivity, competence, and organizational standing of the key validation participants, with the ultimate goal of ascertaining whether those participants have the right incentives to discover and report deficiencies. Internal audit should review validation activities conducted by internal and external parties with the same rigor to see if those activities are being conducted in accordance with this guidance.

External Resources

Although model risk management is an internal process, a bank may decide to engage external resources to help execute certain activities related to the model risk-management framework. These activities could include model validation and review, compliance functions, or other activities in support of internal audit. These resources may provide added knowledge and another level of critical and effective challenge, which may improve the internal model development and risk-management processes. However, this potential benefit should be weighed against the

added costs for such resources and the added time that external parties require to understand internal data, systems, and other relevant bank-specific circumstances.

Whenever external resources are used, the bank should specify the activities to be conducted in a clearly written and agreed-upon scope of work. A designated internal party from the bank should be able to understand and evaluate the results of validation and risk-control activities conducted by external resources. The internal party is responsible for verifying that the agreed upon scope of work has been completed; evaluating and tracking identified issues and ensuring they are addressed; and making sure that completed work is incorporated into the bank's overall model risk-management framework. If the external resources are only utilized to do a portion of validation or compliance work, the bank should coordinate internal resources to complete the full range of work needed. The bank should have a contingency plan in case an external resource is no longer available or is unsatisfactory.

Model Inventory

Banks should maintain a comprehensive set of information for models implemented for use, under development for implementation, or recently retired. While each line of business may maintain its own inventory, a specific party should also be charged with maintaining a firm-wide inventory of all models, which should assist a bank in evaluating its model risk in the aggregate. Any variation of a model that warrants a separate validation should be included as a separate model and cross-referenced with other variations.

While the inventory may contain varying levels of information, given different model complexity and the bank's overall level of model usage, the following are some general guidelines. The inventory should describe the purpose and products for which the model is designed, actual or expected usage, and any restrictions on use. It is useful for the inventory to list the type and source of inputs used by a given model and underlying components (which may include other models), as well as model outputs and their intended use. It should also indicate whether models are functioning properly, provide a description of when they were last updated, and list any exceptions to policy. Other items include the names of individuals responsible for various aspects of the model development and validation; the dates of completed and planned validation activities; and the time frame during which the model is expected to remain valid.

Documentation

Without adequate documentation, model risk assessment and management will be ineffective. Documentation of model development and validation should be sufficiently detailed so that parties unfamiliar with a model can understand how the model operates, its limitations, and its key assumptions. Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses, and exceptions. Developers, users, control and compliance units, and supervisors are all served by effective documentation. Banks can benefit from advances in information and knowledge management systems and electronic documentation to improve the organization, timeliness, and accessibility of the various records and reports produced in the model risk-management process.

Documentation takes time and effort, and model developers and users who know the models well may not appreciate its value. Banks should therefore provide incentives to produce effective and complete model documentation. Model developers should have responsibility during model development for thorough documentation, which should be kept up-to-date as the model and application environment changes. In addition, the bank should ensure that other participants in model risk-management activities document their work, including ongoing monitoring, process verification, benchmarking, and outcomes analysis. Also, line of business or other decision makers should document information leading to selection of a given model and its subsequent validation. For cases in which a bank uses models from a vendor or other third party, it should ensure that appropriate documentation of the third-party approach is available so that the model can be appropriately validated.

Validation reports should articulate model aspects that were reviewed, highlighting potential deficiencies over a range of financial and

economic conditions, and determining whether adjustments or other compensating controls are warranted. Effective validation reports include clear executive summaries, with a statement of model purpose and an accessible synopsis of model and validation results, including major limitations and key assumptions.

CONCLUSION—PART VII

Section 4027.1 provides comprehensive guidance on effective model risk management. Many of the activities described are common industry practice. But all banks should confirm that their practices conform to the principles in this guidance for model development, implementation, and use, as well as model validation. Banks should also ensure that they maintain strong governance and controls to help manage model risk, including internal policies and procedures that appropriately reflect the risk-management principles described in this guidance. Details of model risk-management practices may vary from bank to bank, as practical application of this guidance should be commensurate with a bank's risk exposures, its business activities, and the extent and complexity of its model use.

Many banking organizations (BOs) have substantially increased their securitization activities. Asset securitization typically involves the transfer of potentially illiquid on-balance-sheet assets (for example, loans, leases, and other assets) to a third party or trust. In turn, the third party or trust issues certificates or notes to investors. The cash flow from the transferred assets supports repayment of the certificates or notes. BOs use asset securitization to access alternative funding sources, manage concentrations, improve financial-performance ratios, and more efficiently meet customer needs. Assets typically securitized include credit card receivables and automobile receivable paper, commercial and residential first mortgages, commercial loans, home-equity loans, and student loans.

Managing the risks of securitization activities poses increasing challenges, which may be less obvious and more complex than the risks of traditional lending activities. Securitization can involve credit, liquidity, operational, legal, and reputational risks in concentrations and forms that may not be fully recognized by bank management or adequately incorporated into an institution's risk-management systems. In reviewing these activities, examiners should assess whether BOs fully understand and adequately manage the full range of risks involved in securitization activities.

BOs have been involved with asset-backed securities (ABS), both as investors in them and as major participants in the securitization process. The federal government encourages the securitization of residential mortgages. In 1970, the Government National Mortgage Association (GNMA or Ginnie Mae) created the first publicly traded mortgage-backed security. Shortly thereafter, the Federal National Mortgage Association (Fannie Mae) and the Federal Home Loan Mortgage Corporation (Freddie Mac), both government-sponsored agencies, also developed mortgage-backed securities. The guarantees on the securities that these government or government-sponsored entities provide ensure investors of the payment of principal and interest. These guarantees have greatly facilitated the securitization of mortgage assets. Banks also securitize other types of assets, such as nonperforming loans and lease receivables.

While the objectives of securitization may vary from institution to institution, there are essentially five benefits that can be derived from securitized transactions. First, the sale of assets may reduce regulatory costs. The removal of an asset from an institution's books reduces capital requirements and reserve requirements on the deposits funding the asset. Second, securitization provides originators with an additional source of funding or liquidity. The process of securitization basically converts an illiquid asset into a security with greater marketability. Securitized issues often require a credit enhancement, which results in a higher credit rating than what would normally be obtainable by the institution itself. Consequently, these issues may provide the institution with a cheaper form of funding. Third, securitization may be used to reduce interest-rate risk by improving the institution's asset-liability mix. This is especially true if the institution has a large investment in fixed-rate, low-yield assets. Fourth, by removing assets, the institution enhances its return on equity and assets. Finally, the ability to sell these securities worldwide diversifies the institution's funding base, which reduces the bank's dependence on local economies.

While securitization activities can enhance both credit availability and bank profitability, the risks of these activities must be known and managed. Accordingly, BOs should ensure that their overall risk-management process explicitly incorporates the full range of risks involved in their securitization activities, and examiners should assess whether institutions fully understand and adequately manage these risks. Specifically, examiners should determine whether institutions are recognizing the risks of securitization activities by (1) adequately identifying, quantifying, and monitoring these risks; (2) clearly communicating the extent and depth of these risks in reports to senior management and the board of directors and in regulatory reports; (3) conducting ongoing stress testing to identify potential losses and liquidity needs under adverse circumstances; and (4) setting adequate minimum internal standards for allowances or liabilities for losses, capital, and contingency funding. Incorporating asset-securitization activities into BO's risk-management systems and internal capital-adequacy allocations is particularly important since the current regulatory capital rules may not fully capture the economic substance of the risk exposures arising from many of these activities.

Senior management and directors must have the requisite knowledge of the effect of securitization on the BO's risk profile, and they must be fully aware of the accounting, legal, and risk-based capital nuances of this activity. BOs must fully and accurately distinguish and measure the risks that are transferred versus those that are retained, and they must adequately manage the retained portion. It is essential that BOs engaging in securitization activities have appropriate front- and back-office staffing; internal and external accounting and legal support; audit or independent-review coverage; information systems capacity; and oversight mechanisms to execute, record, and administer these transactions correctly.

Appropriate valuation and modeling methodologies must be used. They must be able to determine the initial and ongoing fair value of retained interests. Accounting rules (generally accepted accounting principles, or GAAP) provide a method to recognize an immediate gain (or loss) on the sale through booking a "retained interest." The carrying value, however, of that interest must be fully documented, based on reasonable assumptions, and regularly analyzed for any subsequent impairment in value. The best evidence of fair value is a quoted market price in an active market. When quoted market prices are not available, accounting rules allow fair value to be estimated. This estimate must be based on the "best information available in the circumstances."[1] An estimate of fair value must be supported by reasonable and current assumptions. If a best estimate of fair value is not practicable, the asset is to be recorded at zero in financial and regulatory reports.

Unforeseen market events that affect the discount rate or performance of receivables supporting a retained interest can swiftly and dramatically alter its value. Without appropriate internal controls and independent oversight, an institution that securitizes assets may inappropriately generate "paper profits" or mask actual losses through flawed loss assumptions, inaccurate prepayment rates, and inappropriate discount rates. Liberal and unsubstantiated assumptions can result in material inaccuracies in financial statements; substantial write-downs of retained interests; and, if retained interests represent an excessive concentration of the sponsoring institution's capital, the institution's demise.

An institution's failure to adequately understand the risks inherent in its securitization activities and to incorporate risks into its risk-management systems and internal capital allocations may constitute an unsafe and unsound banking practice. Furthermore, retained interests that lack objectively verifiable support or that fail to meet these supervisory standards will be classified as loss and disallowed for inclusion as assets of the institution for regulatory capital purposes. (See SR-99-37.) Accordingly, for those institutions involved in asset securitization or providing credit enhancements in connection with loan sales and securitization, examiners should assess whether the institutions' systems and processes adequately identify, measure, monitor, and control *all* the risks involved in its securitization activities. Examiners also will review an institution's valuation of retained interests and the concentration of these assets relative to capital. Consistent with existing supervisory authority, BOs may be required, on a case-by-case basis, to hold additional capital commensurate with their risk exposures.[2] An excessive dependence on securitizations for day-to-day core funding can present significant liquidity problems during times of market turbulence or if there are difficulties specific to the BO.

Traditional lending activities are generally funded by deposits or other liabilities, with both the assets and related liabilities reflected on the balance sheet. Liabilities must generally increase in order to fund additional loans. In contrast, the securitization process generally does not increase on-balance-sheet liabilities in proportion to the volume of loans or other assets securitized. As discussed more fully below, when banking organizations securitize their assets and these transactions are treated as sales, both the assets and the related ABS (liabilities) are removed from the balance sheet. The cash proceeds from the securitization transactions are generally used

1. See Statement of Financial Accounting Standards No. 166, "Accounting for Transfers of Financial Assets, an Amendment of FASB Statement No. 140 (FAS 166)" and Statement of Financial Accounting Standards No. 167, "Amendments to FASB Interpretation No. 146(R) (FAS 167)." Among other things, FAS 166 and FAS 167 modified the accounting treatment under U. S. generally accepted accounting principles of certain structured finance transactions involving a special purpose entity. See also FASB Statement No. 157, "Fair Value Measurements."

2. For instance, an institution that has high concentrations of retained interests relative to its capital or is otherwise at risk from impairment of these assets may be subject to this requirement.

to originate or acquire additional loans or other assets for securitization, and the process is repeated. Thus, for the same volume of loan originations, securitization results in lower assets and liabilities compared with traditional lending activities.

THE SECURITIZATION PROCESS

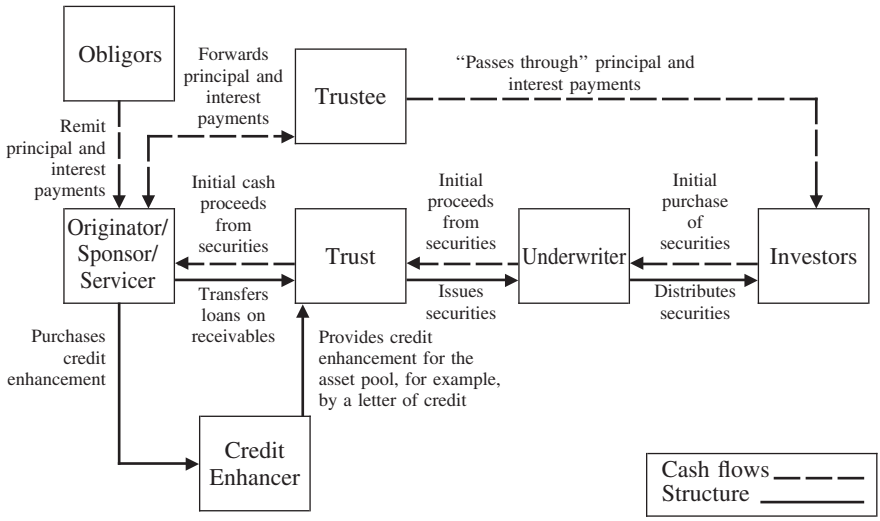
As depicted in figure 1, the asset-securitization process begins with the segregation of loans or leases into pools that are relatively homogeneous with respect to credit, maturity, and interest-rate risks. These pools of assets are then transferred to a trust or other entity known as an issuer because it issues the securities or ownership interests that are acquired by investors. These ABS may take the form of debt, certificates of beneficial ownership, or other instruments. The issuer is typically protected from bankruptcy by various structural and legal arrangements. A sponsor that provides the assets to be securitized owns or otherwise establishes the issuer.

Each issue of ABS has a servicer that is responsible for collecting interest and principal payments on the loans or leases in the underlying pool of assets and for transmitting these funds to investors (or a trustee representing them). A trustee is responsible for monitoring the activities of the servicer to ensure that it properly fulfills its role.

A guarantor may also be involved to ensure that principal and interest payments on the securities will be received by investors on a timely basis, even if the servicer does not collect these payments from the obligors of the underlying assets. Many issues of mortgage-backed securities are either guaranteed directly by GNMA, which is backed by the full faith and credit of the U.S. government, or by Fannie Mae or Freddie Mac, which are government-sponsored agencies that are perceived by the credit markets to have the implicit support of the federal government. Privately issued mortgage-backed securities and other types of ABS generally depend on some form of credit enhancement provided by the originator or third party to insulate the investor from a portion of or all credit losses. Usually, the amount of the credit enhancement is based on several multiples of the historical losses experienced on the particular asset backing the security.

The structure of an asset-backed security and the terms of the investors' interest in the collateral can vary widely depending on the type of collateral, the desires of investors, and the use of credit enhancements. Securitizations typically carve up the risk of credit losses from the

Figure 1—Pass-through, asset-backed securities: structure and cash flows



underlying assets and distribute it to different parties. The *first-dollar,* or most subordinate, loss position is first to absorb credit losses, and the most *senior* investor position is last to absorb losses; there may also be one or more loss positions in between (*second-dollar* loss positions). Each loss position functions as a credit enhancement for the more senior positions in the structure. In other words, when ABS reallocate the risks in the underlying collateral (particularly credit risk), the risks are moved into security tranches that match the desires of investors. For example, senior-subordinated security structures give holders of senior tranches greater credit-risk protection—albeit at lower yields—than holders of subordinated tranches. Under this structure, at least two classes of asset-backed securities, a senior and a junior or subordinated class, are issued in connection with the same pool of collateral. The senior class is structured so that it has a priority claim on the cash flows from the underlying pool of assets. The subordinated class must absorb credit losses on the collateral before losses can be charged to the senior portion. Because the senior class has this priority claim, cash flows from the underlying pool of assets must first satisfy the requirements of the senior class. Only after these requirements have been met will the cash flows be directed to service the subordinated class.

Credit Enhancement

ABS can use various forms of credit enhancements to transform the risk-return profile of underlying collateral. These include third-party credit enhancements, recourse provisions, overcollateralization, and various covenants and indentures. The sponsor of the asset securitization may provide a portion of the total credit enhancement internally, as part of the securitization structure, through the use of excess spread accounts, overcollateralization, retained subordinated interests, or other similar on-balance-sheet assets. When these or other on-balance-sheet internal enhancements are provided, the enhancements are "residual interests" and are a form of recourse.[3]

A seller may also arrange for a third party to provide credit enhancement in an asset securitization. If the third-party enhancement is provided by another bank, the other bank assumes some portion of the assets' credit risk. All forms of third-party enhancements, that is, all arrangements in which a bank assumes credit risk from third-party assets or other claims that it has not transferred, are referred to as *direct-credit substitutes.* The economic substance of a bank's credit risk from providing a direct-credit substitute can be identical to its credit risk from retaining recourse on assets it has transferred. Third-party credit enhancements include standby letters of credit, collateral or pool insurance, or surety bonds from third parties. Many asset securitizations use a combination of recourse and third-party enhancements to protect investors from credit risk. When third-party enhancements are not provided, the selling bank ordinarily retains virtually all of the credit risk on the assets transferred.

Some ABS, such as those backed by credit card receivables, typically use a *spread account.* This account is actually an escrow account. The funds in this account are derived from a portion of the spread between the interest earned on the assets in the underlying pool and the lower interest paid on securities issued by the trust. The amounts that accumulate in the account are used to cover credit losses in the underlying asset pool up to several multiples of historical losses on the particular asset collateralizing the securities. Overcollateralization, a form of credit enhancement covering a predetermined amount of potential credit losses, occurs when the value of the underlying assets exceeds the face value of the securities.

A similar form of credit enhancement is the cash-collateral account, which is established when a third party deposits cash into a pledged account. The use of cash-collateral accounts, which are considered by enhancers to be loans, grew as the number of highly rated banks and other credit enhancers declined in the early 1990s. Cash-collateral accounts eliminate *event risk,* or the risk that the credit enhancer will have its credit rating downgraded or that it will not be able to fulfill its financial obligation to absorb losses and thus provide credit protection to investors in a securitization.

An investment banking firm or other organization generally serves as an underwriter for ABS. In addition, for asset-backed issues that are publicly offered, a credit-rating agency will analyze the policies and operations of the originator and servicer, as well as the structure,

3. Purchased credit-enhancing interest-only strips are also considered "residual interests."

underlying pool of assets, expected cash flows, and other attributes of the securities. Before assigning a rating to the issue, the rating agency will also assess the extent of loss protection provided to investors by the credit enhancements associated with the issue.

TYPES OF ASSET-BACKED SECURITIES

Asset securitization involves different types of capital-market instruments. (For more information, see the *Trading and Capital-Markets Activities Manual,* section 4105.1, "Asset-Backed Securities and Asset-Backed Commercial Paper," and section 4110.1, "Residential Mortgage–Backed Securities.") These instruments may be structured as "pass-throughs" or "pay-throughs." Under a pass-through structure, the cash flows from the underlying pool of assets are passed through to investors on a pro rata basis. This type of security may be a single-class instrument, such as a GNMA pass-through, or a multiclass instrument, such as a real estate mortgage investment conduit (REMIC).[4]

The pay-through structure, with multiple classes, combines the cash flows from the underlying pool of assets and reallocates them to two or more issues of securities that have different cash-flow characteristics and maturities. An example is the collateralized mortgage obligation (CMO), which has a series of bond classes, each with its own specified coupon and stated maturity. In most cases, the assets that make up the CMO collateral pools are pass-through securities. Scheduled principal payments and any prepayments from the underlying collateral go first to the earliest maturing class of bonds. This first class of bonds must be retired before the principal cash flows are used to retire the later bond classes. The development of the pay-through structure resulted from the desire to broaden the marketability of these securities to investors who were interested in maturities other than those generally associated with pass-through securities.

Multiple-class ABS may also be issued as derivative instruments, such as "stripped" securities. Investors in each class of a stripped security will receive a different portion of the principal and interest cash flows from the underlying pool of assets. In their purest form, stripped securities may be issued as interest-only (IO) strips, for which the investor receives 100 percent of the interest from the underlying pool of assets, and as principal-only (PO) strips, for which the investor receives all of the principal.

In addition to these securities, other types of financial instruments may arise as a result of asset securitization, as follows:

- *Servicing assets.* These assets become a distinct asset recorded on the balance sheet when contractually separated from the underlying assets that have been sold or securitized and when the servicing of those assets is retained. (See FAS 140 for more information.) In addition, servicing assets are created when organizations purchase the right to act as servicers for loan pools. The value of the servicing assets is based on the contractually specified servicing fees, net of servicing costs.
- *Interest-only strips receivables.* These cash flows are accounted for separately from servicing assets and reflect the right to future interest income from the serviced assets in excess of the contractually specified servicing fees.
- *ABS residuals.* These residuals (sometimes referred to as "residuals," "residual interests," or "retained interests" represent claims on any cash flows that remain after all obligations to investors and any related expenses have been met. The excess cash flows may arise as a result of overcollateralization or from reinvestment income. Residuals can be retained by sponsors or purchased by investors in the form of securities.

RISKS ASSOCIATED WITH ASSET SECURITIZATION

While clear benefits accrue to banking organizations that engage in securitization activities

4. In the early 1980s, collateralized mortgage obligations (CMOs), or multiple-class securities, were introduced to help minimize the reinvestment and interest-rate risks inherent in the traditional fixed-rate mortgage-backed security. As a result of the Tax Reform Act of 1986, the REMIC was created. The REMIC is a more flexible mortgage security that expanded the appeal of the CMO structure to a wider investor base and offered preferred tax status to both investors and issuers. Today, almost all CMOs are issued in REMIC form. ("The ABCs of CMOs, REMICs and IO/POs: Rocket Science Comes to Mortgage Finance," *Journal of Accountancy*, April 1991, p. 41.)

and invest in ABS, these activities have the potential to increase the overall risk profile of the banking organization if they are not carried out prudently. For the most part, the types of risks that financial institutions encounter in the securitization process are identical to those that they face in traditional lending transactions, including credit risk, concentration risk, interest-rate risk (including prepayment risk), operational risk, liquidity risk, moral-recourse risk, and funding risk. However, since the securitization process separates the traditional lending function into several limited roles, such as originator, servicer, credit enhancer, trustee, and investor, the types of risks that a bank will encounter will differ depending on the role it assumes.

Investor-Specific Risks

Investors in ABS will be exposed to varying degrees of credit risk, that is, the risk that obligors will default on principal and interest payments. Like the investors in the direct investments of the underlying assets, ABS investors are also subject to the risk that the various parties in the securitization structure, for example, the servicer or trustee, will be unable to fulfill their contractual obligations. Moreover, investors may be susceptible to concentrations of risks across various asset-backed security issues (1) through overexposure to an organization that performs various roles in the securitization process or (2) as a result of geographic concentrations within the pool of assets providing the cash flows for an individual issue. Also, since the secondary markets for certain ABS are limited, investors may encounter greater than anticipated difficulties (liquidity risk) when seeking to sell their securities. Furthermore, certain derivative instruments, such as stripped asset-backed securities and residuals, may be extremely sensitive to interest rates and exhibit a high degree of price volatility. Therefore, they may dramatically affect the risk exposure of investors unless used in a properly structured hedging strategy. Examiner guidance in the *Trading and Capital-Markets Activities Manual,* section 3000.1, "Investment Securities and End-User Activities," is directly applicable to ABS held as investments.

Issuer-Specific Risks

Banking organizations that issue ABS may be subject to pressures to sell only their best assets, thus reducing the quality of their own loan portfolios. On the other hand, some banking organizations may feel pressures to relax their credit standards because they can sell assets with higher risk than they would normally want to retain for their own portfolios.

To protect their name in the market, issuers may face pressures to provide "moral recourse" by repurchasing securities backed by loans or leases they have originated that have deteriorated and become nonperforming. Funding risk may also be a problem for issuers when market aberrations do not permit the issuance of asset-backed securities that are in the securitization pipeline.

Servicer-Specific Risks

Banking organizations that service securitization issues must ensure that their policies, operations, and systems will not permit breakdowns that may lead to defaults. Substantial fee income can be realized by acting as a servicer. An institution already has a fixed investment in its servicing systems, and achieving economies of scale relating to that investment is in its best interest. The danger, though, lies in overloading the system's capacity, thereby creating enormous out-of-balance positions and cost overruns. Servicing problems may precipitate a technical default, which in turn could lead to the premature redemption of the security. In addition, expected collection costs could exceed fee income. (For further guidance, examiners should see section 2040.3, "Loan Portfolio Management: Examination Procedures," under the "Loan Portfolio Review and Analysis" heading.)

ACCOUNTING ISSUES

Sale or Borrowing Treatment

Asset-securitization transactions are frequently structured to obtain certain accounting treatments, which in turn affect reported measures of profitability and capital adequacy. In transferring assets into a pool to serve as collateral for ABS, a key question is whether the transfer should be treated as a sale of the assets or as a

collateralized borrowing, that is, a financing transaction secured by assets. Treating these transactions as a sale of assets results in their being removed from the banking organization's balance sheet, thus reducing total assets relative to earnings and capital, and thereby producing higher performance and capital ratios.[5] Treating these transactions as financings, however, means that the assets in the pool remain on the balance sheet and are subject to capital requirements and the related liabilities-to-reserve requirements.[6]

Valuation and Modeling Processes for Retained Interests

The methods and models BOs use to value retained interests and the difficulties in managing exposure to these volatile assets can raise supervisory concerns. Under GAAP, a BO recognizes an immediate gain (or loss) on the sale of assets by recording its retained interest at fair value. The valuation of the retained interest is based on the present value of future cash flows in excess of the amounts needed to service the bonds and cover credit losses and other fees of the securitization vehicle.[7]

Determinations of fair value should be based on reasonable, conservative assumptions about factors such as discount rates, projected credit losses, and prepayment rates. Bank supervisors expect retained interests to be supported by verifiable documentation of fair value in accordance with GAAP. In the absence of such support, the retained interests should not be carried as assets on an institution's books, but should be charged off. Other supervisory concerns include failure to recognize and hold sufficient capital against recourse obligations generated by securitizations, and the absence of an adequate and independent audit function.

The method and key assumptions used to value the retained interests and servicing assets or liabilities must be reasonable and fully documented. The key assumptions in all valuation analyses include prepayment or payment rates, default rates, loss-severity factors, and discount rates. Institutions are expected to take a logical and conservative approach when developing securitization assumptions and capitalizing future income flows. It is important that management quantifies the assumptions at least quarterly on a pool-by-pool basis and maintains supporting documentation for all changes to the assumptions as part of the valuation. Policies should define the acceptable reasons for changing assumptions and require appropriate management approval.

An exception to this pool-by-pool valuation analysis may be applied to revolving-asset trusts if the master-trust structure allows excess cash flows to be shared between series. In a master trust, each certificate of each series represents an undivided interest in all of the receivables in the trust. Therefore, valuations are appropriate at the master-trust level.

To determine the value of the retained interest at inception, and to make appropriate adjustments going forward, the institution must implement a reasonable modeling process to comply with FAS 140. Management is expected to employ reasonable and conservative valuation assumptions and projections, and to maintain verifiable objective documentation of the fair value of the retained interest. Senior management is responsible for ensuring that the valuation model accurately reflects the cash flows according to the terms of the securitization's structure. For example, the model should account for any cash collateral or overcollateralization triggers, trust fees, and insurance payments if appropriate. The board and management are accountable for the model builders' possessing the necessary expertise and technical proficiency to perform the modeling process. Senior management should ensure that internal controls are in place to provide for the ongoing integrity of management information systems (MIS) associated with securitization activities.

As part of the modeling process, the risk-management function should ensure that periodic validations are performed to reduce vulnerability to model risk. Validation of the model includes testing the internal logic, ensuring empirical support for the model assumptions, and back-testing the models using actual cash flows on a pool-by-pool basis. The validation process should be documented to support conclusions. Senior management should ensure the validation process is independent from line man-

5. See FAS 140 for criteria that must be met for the securitization of assets to be accounted for as a sale.

6. Note, however, that the Federal Reserve's Regulation D (12 CFR 204) defines what constitutes a reservable liability of a depository institution. Thus, although a given transaction may qualify as an asset sale for call report purposes, it nevertheless could result in a reservable liability under Regulation D. See the call report instructions for further guidance. Also, see section 3020.1, "Assessment of Capital Adequacy."

7. See FAS 140.

agement and from the modeling process. The audit scope should include procedures to ensure that the modeling process and validation mechanisms are both appropriate for the institution's circumstances and executed consistently with its asset-securitization policy.

Use of Outside Parties

Third parties are often engaged to provide professional guidance and support regarding an institution's securitization activities, transactions, and valuing of retained interests. The use of outside resources does not relieve directors of their oversight responsibility, nor does it relieve senior management of its responsibilities to provide supervision, monitoring, and oversight of securitization activities, particularly the management of the risks associated with retained interests. Management is expected to have the experience, knowledge, and abilities to discharge its duties; understand the nature and extent of the risks that retained interests present; and have the policies and procedures necessary to implement an effective risk-management system to control such risks. Management must have a full understanding of the valuation techniques employed, including the basis and reasonableness of underlying assumptions and projections.

Market Discipline and Disclosures

Transparency through public disclosure is crucial to effective market discipline and can reinforce supervisory efforts to promote high standards in risk management. Timely and adequate information on the institution's asset-securitization activities should be disclosed. The information in the disclosures should be comprehensive; however, the amount of disclosure that is appropriate will depend on the volume of securitizations and complexity of the BO. Well-informed investors, depositors, creditors, and other counterparties can provide a BO with strong incentives for maintaining sound risk-management systems and internal controls. Adequate disclosure allows market participants to better understand the BO's financial condition and apply market discipline, thus creating incentives to reduce inappropriate risk-taking or inadequate risk-management practices. Examples of sound disclosures include—

- accounting policies for measuring retained interests, including a discussion of the impact of key assumptions on the recorded value;
- the process and methodology used to adjust the value of retained interests for changes in key assumptions;
- risk characteristics, both quantitative and qualitative, of the underlying securitized assets;
- the role of retained interests as credit enhancements to special-purpose entities and other securitization vehicles, including a discussion of techniques used for measuring credit risk; and
- sensitivity analyses or stress testing conducted by the BO, showing the effect of changes in key assumptions on the fair value of retained interests.

CAPITAL ADEQUACY

As with all risk-bearing activities, institutions should fully support the risk exposures of their securitization activities with adequate capital. Banking organizations should ensure that their capital positions are sufficiently strong to support *all* the risks associated with these activities on a fully consolidated basis and should maintain adequate capital in all affiliated entities engaged in these activities. The Federal Reserve's risk-based capital guidelines establish *minimum* capital ratios, and those banking organizations exposed to high or above-average degrees of risk are expected to operate significantly *above* the minimum capital standards.

The current regulatory capital rules may not fully incorporate the economic substance of the risk exposures involved in many securitization activities. Therefore, when evaluating capital adequacy, examiners should ensure that banking organizations that (1) sell assets with recourse, (2) assume or mitigate credit risk through the use of credit derivatives, or (3) provide direct-credit substitutes and liquidity facilities to securitization programs are accurately identifying and measuring these exposures and maintaining capital at aggregate levels sufficient to support the associated credit, market, liquidity, reputational, operational, and legal risks.

Examiners should review the substance of securitizations when assessing underlying risk exposures. For example, partial, first-loss direct-

credit substitutes providing credit protection to a securitization transaction can, in substance, involve the same credit risk as would be involved in holding the entire asset pool on the institution's balance sheet. Examiners should ensure that banks have implemented reasonable methods for allocating capital against the economic substance of credit exposures arising from early-amortization events and liquidity facilities associated with securitized transactions. These liquidity facilities are usually structured as short-term commitments in order to avoid a risk-based capital requirement, even though the inherent credit risk may be similar to that of a guarantee.[8]

If, in the examiner's judgment, an institution's capital level is not sufficient to provide protection against potential losses from the above credit exposures, this deficiency should be reflected in the banking organization's CAMELS rating. Furthermore, examiners should discuss the capital deficiency with the institution's management and, if necessary, its board of directors. Such an institution will be expected to develop and implement a plan for strengthening the organization's overall capital adequacy to levels deemed appropriate given all the risks to which it is exposed.

RISK-BASED CAPITAL PROVISIONS AFFECTING ASSET SECURITIZATION

The risk-based capital framework assigns risk weights to loans, ABS, off-balance-sheet credit enhancements, and other assets related to securitization.[9] Second, banks that transfer assets with recourse to the seller as part of the securitization process are explicitly required to hold capital against their off-balance-sheet credit exposures. However, the specific capital requirement will depend on the amount of recourse retained by the transferring institution and the type of asset sold with recourse. Third, banking organizations that provide credit enhancement to asset-securitization issues through standby letters of credit or by other means must hold capital against the related off-balance-sheet credit exposure.

Assigning Risk Weights

The risk weights assigned to an asset-backed security generally depend on the issuer and on whether the assets that compose the collateral pool are mortgage-related assets or assets guaranteed by a U.S. government agency. ABS issued by a trust or single-purpose corporation and backed by nonmortgage assets generally are to be assigned a risk weight of 100 percent.

Securities guaranteed by U.S. government agencies and those issued by U.S. government–sponsored agencies are assigned risk weights of 0 percent and 20 percent, respectively, because of the low degree of credit risk. Accordingly, mortgage pass-through securities guaranteed by GNMA are placed in the risk category of 0 percent. In addition, securities such as participation certificates and CMOs issued by Fannie Mae or Freddie Mac are assigned a 20 percent risk weight.

However, several types of securities issued by Fannie Mae and Freddie Mac are excluded from the lower risk weight and slotted in the 100 percent risk category. Residual interests (for example, CMO residuals) and subordinated classes of pass-through securities or CMOs that absorb more than their pro rata share of loss are assigned to the 100 percent risk-weight category. Furthermore, high-risk mortgage-derivative securities and all stripped, mortgage-backed securities, including IOs, POs, and similar instruments, are assigned to the 100 percent risk-weight category because of their high price volatility and market risk.

A privately issued mortgage-backed security that meets the criteria listed below is considered a direct or indirect holding of the underlying mortgage-related assets and is generally assigned to the same risk category as those assets (for example, U.S. government agency securities, U.S. government–sponsored agency securities, FHA- and VA-guaranteed mortgages, and con-

8. For further guidance on distinguishing, for risk-based capital purposes, whether a facility is a short-term commitment or a direct-credit substitute, see SR-92-11, "Asset-Backed Commercial Paper Programs." Essentially, facilities that provide liquidity, but which also provide credit protection to secondary-market investors, are to be treated as direct-credit substitutes for purposes of risk-based capital.

9. In addition to being subject to risk-based capital requirements, servicing assets are also subject to capital limitations. The total amount of servicing assets (including both mortgage-servicing assets and nonmortgage-servicing assets) and purchased credit-card relationships that may be included in a bank's capital may not, in the aggregate, exceed 100 percent of tier 1 capital. The total amount of nonmortgage-servicing assets and purchased credit-card relationships is subject to a separate aggregate sublimit of 25 percent of tier 1 capital.

ventional mortgages). However, under no circumstances will a privately issued mortgage-backed security be assigned to the 0 percent risk category. Therefore, private issues that are backed by GNMA securities will be assigned to the 20 percent risk category as opposed to the 0 percent category appropriate to the underlying GNMA securities. The criteria that a privately issued mortgage-backed security must meet to be assigned the same risk weight as the underlying assets are as follows:

- The underlying assets are held by an independent trustee, and the trustee has a first-priority, perfected security interest in the underlying assets on behalf of the holders of the security.
- The holder of the security has an undivided pro rata ownership interest in the underlying mortgage assets, or the trust or single-purpose entity (or conduit) that issues the security has no liabilities unrelated to the issued securities.
- The cash flow from the underlying assets of the security in all cases fully meets the cash-flow requirements of the security without undue reliance on any reinvestment income.
- No material reinvestment risk is associated with any funds awaiting distribution to the holders of the security.

Those privately issued mortgage-backed securities that do not meet the above criteria are to be assigned to the 100 percent risk category.

If the underlying pool of mortgage-related assets is composed of more than one type of asset, then the entire class of mortgage-backed securities is assigned to the category appropriate to the highest risk-weighted asset in the asset pool. For example, if the security is backed by a pool consisting of U.S. government–sponsored agency securities (for example, Freddie Mac participation certificates) that qualify for a 20 percent risk weight and conventional mortgage loans that qualify for the 50 percent risk category, then the security would receive the 50 percent risk weight.

While not set forth specifically in the risk-based capital guidelines, securities backed by student loans that meet the above-mentioned criteria may also be considered an indirect holding of the underlying assets and assigned to the same risk category as those assets. For instance, the U.S. Department of Education conditionally guarantees banks originating student loans for 98 percent of each loan under the Federal Family Education Loan Program. The guaranteed portion of the student loans is eligible for the 20 percent risk category. Therefore, senior ABS that are supported solely by student loans that are conditionally guaranteed by the Department of Education and that meet the four criteria listed above may be assigned to the 20 percent risk category to the extent they are guaranteed. As with mortgage-backed securities, subordinated student loan–backed securities and securities backed by pools of conditionally guaranteed and nonguaranteed student loans would be assigned to the 100 percent risk category.

Banks report their activities in accordance with GAAP, which permits asset-securitization transactions to be treated as sales when certain criteria are met even when there is recourse to the seller. In accordance with the RBC guideline, banks are required to hold capital against the off-balance-sheet credit exposure arising from the contingent liability associated with the recourse provisions. This exposure, generally the outstanding principal amount of the assets sold with recourse, is considered a direct-credit substitute that is converted at 100 percent to an on-balance-sheet credit-equivalent amount for appropriate risk weighting.

Recourse Obligations

For regulatory purposes, recourse is generally defined as an arrangement in which an institution retains the risk of credit loss in connection with an asset transfer, if the risk of credit loss exceeds a pro rata share of its claim on the assets.[10] In addition to broad contractual language that may require the seller to support a securitization, recourse can arise from retained interests, retained subordinated security interests, the funding of cash-collateral accounts, or other forms of credit enhancements that place a BO's earnings and capital at risk. These enhancements should generally be aggregated to determine the extent of a BO's support of securitized assets. Although an asset securitization qualifies for sales treatment under GAAP, the underlying assets may still be subject to regulatory risk-

10. See the risk-based capital treatment for sales with recourse at 12 CFR 3, appendix A, section (3)(b)(1)(iii) (for the OCC), and 12 CFR 567.6(a)(2)(i)(c) (for the OTS). For a further explanation of recourse, see the glossary of the call report instructions at "sales of assets for risk-based capital purposes."

based capital requirements. Assets sold with recourse should generally be risk-weighted as if they had not been sold.

Credit-Equivalent Amounts and Risk Weights of Recourse Obligations and Direct-Credit Substitutes

The credit-equivalent amount for a recourse obligation or direct-credit substitute is the full amount of the credit-enhanced assets for which the bank directly or indirectly retains or assumes credit risk, multiplied by a 100 percent conversion factor. A bank that extends a partial direct-credit substitute, for example, a financial standby letter of credit that absorbs the first 10 percent of loss on a transaction, must maintain capital against the full amount of the assets being supported.

To determine the bank's risk-weighted assets for an off-balance-sheet recourse obligation, a third-party direct-credit substitute, or a letter of credit, the credit-equivalent amount is assigned to the risk category appropriate to the obligor in the underlying transaction, after considering any associated guarantees or collateral. For a direct-credit substitute that is an on-balance-sheet asset, for example, a purchased subordinated security, a bank must calculate risk-weighted assets using the amount of the direct-credit substitute and the full amount of the assets it supports, that is, all the more senior positions in the structure. This treatment is subject to the low-level-exposure rule discussed below. (The risk-based capital treatment for asset securitizations is discussed in more detail in section 3020.1.)

If a bank has no claim on a transferred asset, then the retention of any risk of credit loss is recourse. A recourse obligation typically arises when a bank transfers assets and retains an explicit obligation to repurchase the assets or absorb losses due to a default on the payment of principal or interest, or due to any other deficiency in the performance of the underlying obligor or some other party. Recourse may also exist implicitly if a bank provides credit enhancement beyond any contractual obligation to support assets it has sold. The following are examples of recourse arrangements:

- credit-enhancing representations and warranties made on the transferred assets
- loan-servicing assets retained under an agreement that requires the bank to be responsible for credit losses associated with the loans being serviced (mortgage-servicer cash advances that meet the conditions of section III.B.3.a.viii. of the capital adequacy guidelines (12 CFR 208, appendix A) are not recourse arrangements)
- retained subordinated interests that absorb more than their pro rata share of losses from the underlying assets
- assets sold under an agreement to repurchase, if the assets are not already included on the balance sheet
- loan strips sold without contractual recourse when the maturity of the transferred loan is shorter than the maturity of the commitment under which the loan is drawn
- credit derivatives issued that absorb more than the bank's pro rata share of losses from the transferred assets
- clean-up calls at inception that are greater than 10 percent of the balance of the original pool of transferred loans (clean-up calls that are 10 percent or less of the original pool balance and that are exercisable at the option of the bank are not recourse arrangements)

The risk-based capital treatment for asset securitizations is discussed in detail in section 3020.1. In general, a multilevel, ratings-based approach is used to assess the capital requirements on recourse obligations, residual interests (except credit-enhancing interest-only (I/O) strips), direct-credit substitutes, and senior and subordinated securities in asset securitizations, based on their relative exposure to credit risk. Credit ratings from rating agencies are used to measure relative exposure to credit risk and to determine the associated risk-based capital requirement. The Federal Reserve is relying on these credit ratings to make determinations of credit quality for the regulatory capital treatment for loss positions that represent different gradations of credit risk, the same as investors and other market participants. As discussed later in this section, residual interests are subject to (1) a dollar-for-dollar capital charge and (2) a 25 percent of tier 1 capital concentration limit on a subset of residual interests, credit-enhancing I/O strips.

Implicit Recourse Provided to Asset Securitizations

Implicit recourse arises when a bank provides

credit support to one of more of its securitizations beyond its contractual obligation. Implicit recourse, like contractual recourse, exposes an institution to the risk of loss arising from deterioration in the credit quality of the underlying assets of the securitization. Implicit recourse is of supervisory concern because it demonstrates that the securitizing institution is reassuming risk associated with the securitized assets—risk that the institution initially transferred to the marketplace. For risk-based capital purposes, banks deemed to be providing implicit recourse are generally required to hold capital against the entire outstanding amount of assets sold, as though the assets remained on the bank's books.

Banks have typically provided implicit recourse in situations where the originating bank perceived that the failure to provide this support, even though not contractually required, would damage its future access to the asset-backed securities market. An originating bank can provide implicit recourse in a variety of ways. The ultimate determination as to whether implicit recourse exists depends on the facts. The following actions point to a finding of implicit recourse:

- selling assets to a securitization trust or other special-purpose entity (SPE) at a discount from the price specified in the securitization documents, which is typically par value
- purchasing assets from a trust or other SPE at an amount greater than fair value
- exchanging performing assets for nonperforming assets in a trust or other SPE
- funding credit enhancements[10a] beyond contractual requirements

By providing implicit recourse, a bank signals to the market that it still holds the risks inherent in the securitized assets, and, in effect, the risks have not been transferred. Accordingly, examiners must be attentive to banks that provide implicit support, given the risk these actions pose to a bank's financial condition. Increased attention should be given to situations where a bank is more likely to provide implicit support.

Particular attention should be paid to revolving securitizations, such as those used for credit card lines and home equity lines of credit, in which receivables generated by the lines are sold into the securitizations. These securitizations typically provide that, when certain performance criteria hit specified thresholds, no new receivables can be sold into the securitization, and the principal on the bonds issued will begin to pay out. These early-amortization events are intended to protect investors from further deterioration in the underlying asset pool. Once an early-amortization event has occurred, the bank could have difficulties using securitization as a continuing source of funding and, at the same time, have to fund the new receivables generated by the lines of credit on its balance sheet. Thus, banks have an incentive to avoid early amortization by providing implicit support to the securitization.

Examiners should be alert for securitizations that are approaching early-amortization triggers, such as a decrease in the excess spread[10b] below a certain threshold or an increase in delinquencies beyond a certain rate. Providing implicit recourse can pose a degree of risk to a bank's financial condition and to the integrity of its regulatory and public financial statements and reports. Examiners should review securitization documents (for example, pooling and servicing agreements) to ensure that the selling institution limits any post-sale support to that specified in the terms and conditions in the securitization documents. Examiners should also review a sample of receivables transferred between the seller and the trust to ensure that these transfers were conducted in accordance with the contractual terms of the securitization, particularly in cases where the overall credit quality of the securitized loans or receivables has deteriorated. While banks are not prohibited from providing implicit recourse, such support will generally result in higher capital requirements.

Examiners should recommend that prompt supervisory action be taken when implicit recourse is identified. To determine the appropriate action, examiners need to understand the bank's reasons for providing support and the extent of the impact of this support on the bank's earnings and capital. As with contractual recourse, actions involving noncontractual post-sale credit enhancement generally result in the requirement that the bank hold risk-based capital against the entire outstanding amount of the

10a. Credit enhancements include retained subordinated interests, asset-purchase obligations, overcollateralization, cash-collateral accounts, spread accounts, and interest-only strips.

10b. Excess spread generally is defined as finance-charge collections minus certificate interest, servicing fees, and charge-offs allocated to the series.

securitized assets. Supervisors may require the bank to bring all assets in existing securitizations back on the balance sheet for risk-based capital purposes, as well as require the bank to increase its minimum capital ratios. Supervisors may also prevent a bank from removing assets from its risk-weighted asset base on future transactions until the bank demonstrates its intent and ability to transfer risk to the marketplace. In addition, supervisors may consider other actions to ensure that the risks associated with implicit recourse are adequately reflected in the capital ratios. For example, supervisors may require the bank to deduct residual interests from tier 1 capital as well as hold risk-based capital on the underlying assets.

The following examples illustrate post-sale actions that banks have taken on assets they have securitized. These examples are intended to provide guidance on whether these actions would be considered implicit recourse for risk-based capital and other supervisory purposes. A key factor in each scenario and analysis is the potential risk of loss the bank's earnings and capital may be exposed to as a result of its actions.

Account removal: Example 1a

Facts. A bank originates and services credit card receivables throughout the country. The bank decides to divest those credit card accounts of customers who reside in specific geographic areas where the bank lacks a significant market presence. To achieve the maximum sales price, the sale must include both the credit card relationships and the receivables. Because many of the credit card receivables are securitized through a master-trust structure, the bank needs to remove the receivables from the trust. The affected receivables are not experiencing any unusual performance problems. In that respect, the charge-off and delinquency ratios for the receivables to be removed from the trust are substantially similar to those for the trust as a whole.

The bank enters into a contract to sell the specified credit card accounts before the receivables are removed from the trust. The terms of the transaction are arm's length, wherein the bank will sell the receivables at market value. The bank separately agrees to purchase the receivables from the trust at this same price. Therefore, no loss is incurred as a result of removing the receivables from the trust. The bank will only remove receivables from the trust that are due from customers located in the geographic areas where the bank lacks a significant market presence, and it will remove all such receivables from the trust.

Analysis. The removal of the above-described receivables from the trust does not constitute implicit recourse for regulatory capital purposes. Supporting factors for this conclusion include the following:

- The bank's earnings and capital are not exposed to actual or potential risk of loss as a result of removing the receivables from the trust.
- There is no indication that the receivables are removed from the trust because of performance concerns.
- The bank is removing the receivables from the trust for a legitimate business purpose other than to systematically improve the quality of the trust's assets. The legitimate business purpose is evidenced by the bank's prearranged, arm's-length sale agreement that facilitates exiting the business in identified geographic locations.

Examiners should review the terms and conditions of the transaction to ensure that the market value of the receivables is documented and well supported before concluding that this transaction does not represent implicit recourse. Examiners should also ensure that the selling bank has not provided the purchaser with any guarantees or credit enhancements on the sold receivables.

Account removal: Example 1b

Facts. After the establishment of a master trust for a pool of credit card receivables, the receivables in the trust begin to experience adverse performance. A combination of lower-than-expected yields and higher-than-anticipated charge-offs on the pool causes spreads to compress significantly (although not to zero). The bank's internally generated forecasts indicate that spreads will likely become negative in the near future.

Management takes action to support the trust by purchasing the low-quality (delinquent) receivables from the trust at par, although their market value is less than par. The receivables purchased from the trust represent approximately one-third of the trust's total receivables.

This action improves the overall performance of the trust and avoids a potential early-amortization event.

Analysis. The purchase of low-quality receivables from a trust at par constitutes implicit recourse for regulatory capital purposes. The purchase of low-quality receivables at an above-market price exposes the bank's earnings and capital to potential future losses from assets that had previously been sold. Accordingly, the bank is required to hold risk-based capital for the remaining assets in the trust as if they were retained on the balance sheet, as well as hold capital for the assets that were repurchased.

Additions of future assets or receivables: Example 2a

Facts. Months after the issuance of credit card asset-backed securities, charge-offs and delinquencies on the underlying pool of receivables rise dramatically. A rating agency places the securities on watch for a potential rating downgrade, causing the bank to negotiate additional credit support for the securitized assets. The securitization documents require the bank to transfer new receivables to the securitization trust at par value. However, to maintain the rating on the securities, the bank begins to sell replacement receivables into the trust at a discount from par value.

Analysis. The sale of receivables to the trust at a discount constitutes implicit recourse for regulatory capital purposes. The sale of assets at a discount from the price specified in the securitization documents, par value in this example, exposes earnings and capital to future losses. The bank must hold regulatory capital against the outstanding assets in the trust.

Additions of future assets or receivables: Example 2b

Facts. A bank established a credit card master trust. The receivables from the accounts placed in the trust were, on average, of lesser quality than the receivables from accounts retained on the bank's balance sheet. Under the criteria for selecting the receivables to be transferred to the master trust, the bank was prevented from including the better-performing affinity accounts in the initial pool of accounts because the affinity-relationship contract was expiring. The bank and the affinity client subsequently revised the terms of their contract, enabling the affinity accounts to meet the selection criteria and be included in future securitization transactions. Later, rising charge-offs within the pool of receivables held by the trust caused spread compression in the trust. To improve the performance of the assets in the trust, the bank begins to include the better-performing and now-eligible receivables from the affinity accounts among the receivables sold to the trust. This action improves the trust's performance, including its spread levels and charge-off ratios. However, the replacement assets were sold at par in accordance with the terms of the trust agreement, so no current or future charge to the bank's earnings or capital will result from these asset sales. As another result of this action, the performance of the trust's assets closely tracks the credit card receivables that remain on the bank's balance sheet.

Analysis. The actions described above do not constitute implicit recourse for regulatory capital purposes. The bank did not incur any additional risk to earnings or capital after the affinity accounts met the selection criteria for replacement assets and after the associated receivables were among the receivables sold to the trust. The replacement assets were sold at par in accordance with the terms of the trust agreement, so no future charge to earnings or capital will result from these asset sales. The sale of replacement assets into a master-trust structure is part of normal trust management.

In this example, the credit card receivables that remain on the bank's balance sheet closely track the performance of the trust's assets. Nevertheless, examiners should ascertain whether a securitizing bank sells disproportionately higher-quality assets into securitizations while retaining comparatively lower-quality assets on its books; if so, examiners should consider the effect of this practice on the bank's capital adequacy.

Additions of future assets or receivables: Example 2c

Facts. A bank establishes a credit card master trust composed of receivables from accounts that were generally of lower quality than the receivables retained on the bank's balance sheet. The difference in the two portfolios is primarily due to logistical and operational problems that

prevent the bank from including certain better-quality affinity accounts in the initial pool from which accounts were selected for securitization. Rising charge-offs and other factors later result in margin compression on the assets in the master trust, which causes some concern in the market regarding the stability of the outstanding asset-backed securities. A rating agency places several securities on its watch list for a potential rating downgrade. In response to the margin compression, as part of the bank's contractual obligations, spread accounts are increased for all classes by trapping excess spread in conformance with the terms and conditions of the securitization documents. To stabilize the quality of the receivables in the master trust as well as to preclude a downgrade, the bank takes several actions beyond its contractual obligations:

- Affinity accounts are added to the pool of receivables eligible for inclusion in the trust. This change results in improved overall trust performance. However, these receivables are sold to the trust at par value, consistent with the terms of the securitization documents, so no current or future charge to the bank's earnings or capital will result from these asset sales.
- The charge-off policy for cardholders that have filed for bankruptcy is changed from criteria that were more conservative than industry standards and the FFIEC Uniform Retail Credit Classification and Account Management Policy to criteria that conform to industry standards and the FFIEC's policy.
- Charged-off receivables held by the trust are sold to a third party. The funds generated by this sale, effectively accelerating the recovery on these receivables, improve the trust's spread performance.

Analysis. The actions described above do not constitute implicit recourse for regulatory capital purposes. None of the noncontractual actions results in a loss or exposes the bank's earnings or capital to the risk of loss. Because of the margin compression, the bank is obligated to increase the spread accounts in conformance with the terms and conditions of the securitization documents. To the extent this results in an increase in the value of the subordinated spread accounts (residual interests) on the bank's balance sheet, the bank will need to hold additional capital on a dollar-for-dollar basis for the additional credit risk it retains. In contrast, if the bank increased the spread accounts beyond its contractual obligation under the securitization documents in order to provide additional protection to investors, this action would be considered a form of implicit recourse. None of the other actions the bank took would affect the bank's earnings or capital:

- Like other additions to credit card trusts, the additions of receivables from the new affinity accounts were made at par value, in accordance with the securitization documents. Therefore, the addition of receivables to the new affinity accounts would not affect the bank's earnings or capital.
- The trust's policy on the timing of charge-offs on accounts of cardholders who have filed for bankruptcy was changed to meet the less-stringent standards of the industry and those required under the Federal Reserve's policy to improve trust performance, at least temporarily. Nonetheless, this would not affect the bank's earnings or capital.
- In accordance with the securitization documents, proceeds from recoveries on charged-off accounts are the property of the trust. These and other proceeds would continue to be paid out in accordance with the pooling and servicing agreement. No impact on the bank's earnings or capital would result.

Modification of loan-repayment terms: Example 3

Facts. In performing the role of servicer for its securitization, a bank is authorized under its pooling and servicing agreement to modify loan-repayment terms when it appears that this action will improve the likelihood of repayment on the loan. These actions are part of the bank's process of working with customers who are delinquent or otherwise experiencing temporary financial difficulties. All of the modifications are consistent with the bank's internal loan policy. However, in modifying the loan terms, the contractual maturity of some loans may be extended beyond the final maturity date of the most junior class of securities sold to investors. When this occurs, the bank repurchases these loans from the securitization trust at par.

Analysis. The modification of terms and repurchase of loans held by the trust constitutes implicit recourse for regulatory capital pur-

poses. The combination of the loan-term modification for securitized assets and the subsequent repurchase constitutes implicit recourse. While the modification of loan terms is permitted under the pooling and servicing agreement, the repurchase of loans with extended maturities at par exposes the bank's earnings and capital to potential risk of loss.

Servicer's payment of deficiency balances: Example 4

Facts. A wholly owned subsidiary of a bank originates and services a portfolio of home equity loans. After liquidation of the collateral for a defaulted loan, the subsidiary makes the trust whole in terms of principal and interest if the proceeds from the collateral are not sufficient. However, there is no contractual commitment that requires the subsidiary to support the pool in this manner. The payments made to the trust to cover deficient balances on the defaulted loans are not recoverable under the terms of the pooling and servicing agreement.

Analysis. The subsidiary's action constitutes implicit recourse to the bank for regulatory capital purposes. This action is considered implicit recourse because it adversely affects the bank's earnings and capital since the bank absorbs losses on the loans resulting from the actions taken by its subsidiary. Further, no mechanism exists to provide for, and ensure that, the subsidiary will be reimbursed for the payments made to the trust. In addition, examiners will consider any servicer advance a credit enhancement if the servicer is not entitled to full reimbursement[10c] or if the reimbursement is subordinate to other claims.

Reimbursement of credit enhancer's actual losses: Example 5

Facts. A bank sponsoring a securitization arranges for an unrelated third party to provide a first-loss credit enhancement, such as a financial standby letter of credit that will cover losses up to the first 10 percent of the securitized assets. The bank agrees to pay a fixed amount as an annual premium for this credit enhancement. The third party initially covers actual losses that occur in the underlying asset pool in accordance with its contractual commitment under the letter of credit. Later, the selling bank agrees not only to pay the credit enhancer the annual premium on the credit enhancement, but also to reimburse the credit enhancer for the losses it absorbed during the preceding year. This reimbursement for actual losses was not originally provided for in the contractual arrangement between the bank and the credit-enhancement provider.

Analysis. The selling bank's subsequent reimbursement of the credit-enhancement provider's losses constitutes implicit recourse because the bank's reimbursement of losses went beyond its contractual obligations. Furthermore, the Federal Reserve would consider any requirement contained in the original credit-enhancement contract that obligates the bank to reimburse the credit-enhancement provider for its losses to be a recourse arrangement.

Low-Level Exposure

Securitization transactions involving recourse may be eligible for "low-level-recourse" treatment.[11] A bank that contractually limits its maximum off-balance-sheet recourse obligation or direct-credit substitute (except credit-enhancing I/O strips) to an amount less than the effective risk-based capital requirement for the enhanced assets is required to hold risk-based capital equal to the maximum contractual exposure, [12] less any recourse liability established in accordance with GAAP. The low-level-recourse capital treatment thus applies to transactions accounted for as sales under GAAP. The low-level-exposure rule provides that the dollar amount of risk-based capital required for assets transferred with recourse should not exceed the maximum dollar amount for which a bank is contractually liable, less any recourse liability account established in accordance with GAAP. The limitation does not apply when the bank provides credit enhancement beyond any con-

10c. A servicer advance will also be considered a form of credit enhancement if, for any one loan, nonreimbursable advances are not contractually limited to an insignificant amount of that loan's outstanding principal.

11. See the Federal Reserve's Regulation H, appendix A. See also 60 *Fed. Reg.* 17986, April 10, 1995 (OCC); 60 *Fed. Reg.* 8177, February 13, 1995 (FRB); and 60 *Fed. Reg.* 15858, March 28,1995 (FDIC). The OTS low-level-recourse rule is found at 12 CFR 567.6(a)(2)(i)(c).

12. For example, the effective risk-based capital requirement generally would be 4 percent for residential mortgages and 8 percent for commercial loans.

tractual obligation to support assets it has sold. The low-level capital treatment applies to low-level-recourse transactions involving all types of assets, including commercial loans and residential mortgages.

Low-level-recourse transactions can arise when a bank sells or securitizes assets and uses contractual cash flows, such as spread accounts and I/O strips receivables, as a credit enhancement for the sold or securitized assets. A spread account is an escrow account that a bank typically establishes to absorb losses on receivables it has sold in a securitization, thereby providing credit enhancement to investors in the securities backed by the receivables, for example, credit card receivables. As defined in paragraph 14 of FAS 140, an I/O strip receivable is the contractual right to receive some or all of the interest due on a bond, a mortgage loan, or other interest-bearing financial assets. I/O strips are to be measured at fair value with gains or losses recognized either in earnings (if classified as trading) or a separate component of shareholders' equity (if classified as available-for-sale). Paragraph 14 of FAS 140 states that I/O strips, retained interests in securitizations, loans, other receivables, or other financial assets that can contractually be prepaid or otherwise settled in such a way that the holder would not recover substantially all of its recorded investment (except for instruments that are within the scope of Statement of Financial Accounting Standards No. 133 (FAS 133), "Accounting for Derivative Instruments and Hedging Activities," shall be subsequently measured like investments in debt securities classified as available-for-sale or trading under Statement of Financial Accounting Standards No. 115 (FAS 115), "Accounting for Certain Investments in Debt and Equity Securities." Retained interests that lack objectively verifiable support or that fail to meet the supervisory standards (discussed previously in this section) will be classified as loss and disallowed as assets of the BO for regulatory capital purposes.

Another divergence from the general risk-based capital treatment for assets sold with recourse concerns small-business obligations. Qualifying institutions that transfer small-business obligations with recourse are required, for risk-based capital purposes, to maintain capital against only the amount of recourse retained, provided two conditions are met. First, the transactions must be treated as a sale under GAAP. Second, the transferring institutions must establish, pursuant to GAAP, a noncapital reserve sufficient to meet the reasonably estimated liability under their recourse arrangements.

Banking organizations will be considered qualifying institutions for the purpose of treatment of recourse for small-business organizations if, pursuant to the Board's prompt-corrective-action regulation (12 CFR 208.40), they are well capitalized or, by order of the Board, adequately capitalized.[13] To qualify, an institution must be determined to be well capitalized or adequately capitalized without taking into account the preferential capital treatment for any previous transfers of small-business obligations with recourse. The total outstanding amount of recourse retained by a qualifying BO on transfers of small-business obligations receiving the preferential capital treatment cannot exceed 15 percent of the institution's total risk-based capital.

Standby Letters of Credit

Banking organizations that issue standby letters of credit as credit enhancements for ABS issues must hold capital against these contingent liabilities under the risk-based capital guidelines. According to the guidelines, financial standby letters of credit are direct-credit substitutes. A direct-credit substitute is an arrangement in which a bank assumes, in form or substance, credit risk associated with an on- or off-balance-sheet credit exposure that it did not previously own (a third-party asset), and the risk assumed by the bank exceeds the pro rata share of its interest in the third-party asset. If the bank has no claim on the third-party asset, then its

13. Under 12 CFR 208.43, a state member bank is deemed to be well capitalized if it (1) has a total risk-based capital ratio of 10.0 percent or greater; (2) has a tier 1 risk-based capital ratio of 6.0 percent or greater; (3) has a leverage ratio of 5.0 percent or greater; and (4) is not subject to any written agreement, order, capital directive, or prompt-corrective-action directive issued by the Board pursuant to section 8 of the FDI Act, the International Lending Supervision Act of 1983, or section 38 of the FDI Act or any regulation thereunder to meet and maintain a specific capital level for any capital measure.

A state member bank is deemed to be adequately capitalized if it (1) has a total risk-based capital ratio of 8.0 or greater, (2) has a tier 1 risk-based capital ratio of 4.0 percent or greater, (3) has a leverage ratio of 4.0 percent or greater or a leverage ratio of 3.0 percent or greater if the bank is rated composite 1 under the CAMELS rating system in its most recent examination and is not experiencing or anticipating significant growth, and (4) does not meet the definition of a well-capitalized bank.

assumption of *any* credit risk with respect to the third-party asset is a direct-credit substitute. Direct-credit substitutes are converted in their entirety to credit-equivalent amounts. The credit-equivalent amounts are then risk-weighted according to their credit rating, like other direct-credit substitutes, and the risk weight for the corresponding credit rating.

Concentration Limits Imposed on Residual Interests

The creation of a residual interest (the debit) typically results in an offsetting gain on sale (the credit), and thus the generation of an asset. Banking organizations that securitize high-yielding assets with long durations may create a residual-interest asset value that exceeds the risk-based capital charge that would be in place if it had not sold the assets. Serious problems can arise for those banking organizations that distribute earnings too generously, only to be faced later with a downward valuation and charge-off of part or all of the residual interests.

Under the Federal Reserve's capital adequacy guidelines, there is a dollar-for-dollar capital charge on residual interests and a concentration limit on a subset of residual interests, credit-enhancing I/O strips. These strips include any on-balance-sheet assets that represent a contractual right to receive some or all of the interest due on transferred assets, after taking into account trustee and other administrative expenses, interest payments to investors, servicing fees, reimbursements to investors for losses attributable to beneficial interests they hold, and reinvestment income and ancillary revenues (for example, late fees) on the transferred assets. Credit-enhancing I/O strips expose the bank to more than its pro rata share of credit risk and are limited to 25 percent of tier 1 capital, whether they are retained or purchased. Any amount of credit-enhancing I/O strips that exceeds the 25 percent limit will be deducted from tier 1 capital and assets. An example of the concentration calculation required for banks that hold credit-enhancing I/O strips is described below.

A bank has purchased and retained on its balance sheet credit-enhancing I/O strips with a face amount of $100, and it has tier 1 capital of $320 (before any disallowed servicing assets, disallowed purchased credit-card relationships, disallowed credit-enhancing I/O strips, disallowed deferred tax assets, and amounts of nonfinancial equity investments required to be deducted). To determine the amount of credit-enhancing I/O strips that fall within the concentration limit, the bank would multiply the tier 1 capital of $320 by 25 percent, which is $80. The amount of credit-enhancing I/O strips that exceeds the concentration limit, in this case $20, is deducted from tier 1 capital for risk-based and leverage capital calculations and from assets.

Credit-enhancing I/O strips that are not deducted from tier 1 capital (that is, the remaining $80 in the above example), along with all other residual interests not subject to the concentration limit, are subject to a dollar-for-dollar capital requirement. Banks are not required to hold capital for more than 100 percent of the amount of the residual interest. Credit-enhancing I/O strips are not aggregated with any servicing assets or purchased credit-card relationships for purposes of calculating the 25 percent concentration limit.

Continuing the above illustration, once a bank deducts the $20 in disallowed credit-enhancing I/O strips, it must hold $80 in total capital for the $80 that represents the credit-enhancing I/O strips not deducted from tier 1 capital. The $20 deducted from tier 1 capital, plus the $80 in total risk-based capital required under the dollar-for-dollar treatment, equals $100, the face amount of the credit-enhancing I/O strips. Banks may apply a net-of-tax approach to any credit-enhancing I/O strips that have been deducted from tier 1 capital, as well as to the remaining residual interests subject to the dollar-for-dollar treatment. A bank is permitted, but not required, to net the deferred tax liabilities recorded on its balance sheet, if any, that are associated with the residual interests. This netting of the deferred tax liabilities may result in a bank's holding less than 100 percent capital against residual interests.

Normally, a sponsor will eventually receive any excess cash flow remaining from securitizations after investor interests have been met. As previously stated, residual interests are vulnerable to sudden and sizeable write-downs that can hinder a bank's access to the capital markets; damage its reputation in the marketplace; and, in some cases, threaten its solvency. An institution's board of directors and management are expected to develop and implement policies

that limit the amount of residual interests that may be carried as a percentage of total equity capital, based on the results of their valuation and modeling processes. Well-constructed internal limits also lessen the incentives for an institution's personnel to engage in activities designed to generate near-term "paper profits" that may be at the expense of the institution's long-term financial position and reputation.

Asset-Backed Commercial Paper Programs

Although banks' involvement in the securitization of commercial paper has increased significantly over time, asset-backed commercial paper programs differ from other methods of securitization. One difference is that more than one type of asset may be included in the receivables pool.[14] Moreover, in certain cases, the cash flow from the receivables pool may not necessarily match the payments to investors because the maturity of the underlying asset pool does not always parallel the maturity of the structure of the commercial paper. Consequently, when the paper matures, it is usually rolled over or funded by another issue. In certain circumstances, a maturing issue of commercial paper cannot be rolled over. To address this problem, many banks have established backup liquidity facilities. Certain banks have classified these backup facilities as pure liquidity facilities, despite the credit-enhancement element present in them, and, as a result, have incorrectly assessed the risks associated with these facilities. In these cases, the backup liquidity facilities have been more similar to direct-credit substitutes than to loan commitments.

An asset-backed commercial paper (ABCP) program typically is a program through which a bank provides funding to its corporate customers by sponsoring and administering a bankruptcy-remote special-purpose entity that purchases asset pools from, or extends loans to, those customers.[15] The asset pools in an ABCP program might include, for example, trade receivables, consumer loans, or ABS. The ABCP program raises cash to provide funding to the bank's customers through the issuance of externally rated commercial paper into the market. Typically, the sponsoring bank provides liquidity and credit enhancements to the ABCP program. These enhancements aid the program in obtaining high credit ratings that facilitate the issuance of the commercial paper.[16]

Banks consolidating ABCP program assets must include all of the program assets (mostly receivables and securities) and liabilities (mainly commercial paper) on their balance sheets for purposes of the bank Reports of Condition and Income (Call Reports).

Sponsoring BOs generally face limited risk exposure to ABCP programs. This risk usually is confined to the credit enhancements and liquidity-facility arrangements that sponsoring BOs provide to these programs. In addition, operational controls and structural provisions, along with overcollateralization or other credit enhancements provided by the companies that sell assets into ABCP programs, mitigate the risks to which sponsoring BOs are exposed.

Liquidity facilities supporting ABCP. Liquidity facilities supporting ABCP often take the form of commitments to lend to, or to purchase assets from, any structure, program, or conduit in the event that funds are needed to repay maturing commercial paper. Typically, this need for liquidity is due to a timing mismatch between cash collections on the underlying assets in the program and scheduled repayments of the commercial paper issued by the program.

A bank that provides liquidity facilities to ABCP is exposed to credit risk, regardless of the term of the liquidity facilities. For example, an ABCP program may require a liquidity facility to purchase assets from the program at the first sign of deterioration in the credit quality of an asset pool, thereby removing such assets from the program. In such an event, a draw on the liquidity facility exposes the bank to credit risk.

14. See the Federal Reserve System's Supervision and Regulation Task Force on Securitization, "An Introduction to Asset Securitization," issued as an attachment to SR-90-16. See also "Asset-Backed Commercial Paper Programs," *Federal Reserve Bulletin*, February 1992.

15. The definition of *ABCP program* generally includes structured investment vehicles (entities that earn a spread by issuing commercial paper and medium-term notes and using the proceeds to purchase highly rated debt securities) and securities arbitrage programs.

16. A bank is considered the *sponsor of an ABCP program* if it establishes the program; approves the sellers permitted to participate in the program; approves the asset pools to be purchased by the program; or administers the program by monitoring the assets, arranging for debt placement, compiling monthly reports, or ensuring compliance with the program documents and with the program's credit and investment policy.

Short-term commitments with an original maturity of one year or less expose banks to a lower degree of credit risk than longer-term commitments. This difference in the degree of credit risk is reflected in the risk-based capital requirement for the different types of exposures through liquidity facilities.

The Board's risk-based capital guidelines impose a 10 percent credit-conversion factor on unused portions of eligible short-term liquidity facilities supporting ABCP. Under the risk-based capital guidelines and the Board's interpretations thereof, the credit conversion factor for an eligible ABCP liquidity facility is based on whether the facility has an original maturity of one year or less.[17] A 50 percent credit-conversion factor applies to eligible ABCP liquidity facilities having a maturity greater than one year. To be an eligible ABCP liquidity facility and qualify for the 10 or 50 percent credit-conversion factor, the facility must be subject to an asset quality test at the time of inception that does not permit funding against (1) assets that are 90 days or more past due, (2) assets that are in default, and (3) assets or exposures that are externally rated below investment grade at the time of funding if the assets or exposures were externally rated at the inception of the facility. However, a liquidity facility may also be an eligible liquidity facility if it funds against assets that are guaranteed—either conditionally or unconditionally—by the U.S. government, U.S. government agencies, or by an OECD central government, regardless of whether the assets are 90 days past due, in default, or externally rated investment grade.

The 10 or 50 percent credit-conversion factors apply, regardless of whether the structure issuing the ABCP meets the rule's definition of an ABCP program. For example, a capital charge would apply to an eligible short-term liquidity facility that provides liquidity support to ABCP where the ABCP constitutes less than 50 percent of the securities issued by the program, thus causing the issuing structure not to meet the rule's definition of an ABCP program. However, if a bank (1) does not meet this definition and must include the program's assets in its risk-weighted asset base or (2) otherwise chooses to include the program's assets in risk-weighted assets, then no risk-based capital requirement will be assessed against any liquidity facilities provided by the bank that support the program's ABCP. Ineligible liquidity facilities will be treated as recourse obligations or direct-credit substitutes for the purposes of the Board's risk-based capital guidelines.

The Board's risk-based capital guidelines do not specifically mandate, authorize, or prohibit a look-through approach to eligible ABCP liquidity facilities. The Federal Reserve and other federal banking agencies have taken the position that a risk weight may be applied to the credit equivalent amount of an eligible ABCP liquidity facility by looking through to the underlying assets of the ABCP conduit after considering any collateral or guarantees, or external credit ratings, if applicable. For example, if an eligible short-term liquidity facility providing liquidity support to ABCP covered an asset-backed security (ABS) externally rated AAA, then the notional amount of the liquidity facility would be converted at 10 percent to an on-balance-sheet credit-equivalent amount and assigned to the 20 percent risk-weight category appropriate for AAA-rated ABS.

Overlapping exposures to an ABCP program. A bank may have multiple overlapping exposures to a single ABCP program (for example, both a program-wide credit enhancement and multiple pool-specific liquidity facilities to an ABCP program that is not consolidated for risk-based capital purposes). A bank must hold risk-based capital only once against the assets covered by the overlapping exposures. Where the overlapping exposures are subject to different risk-based capital requirements, the bank must apply the risk-based capital treatment that results in the highest capital charge to the overlapping portion of the exposures.

For example, assume a bank provides a program-wide credit enhancement that would absorb 10 percent of the losses in all of the underlying asset pools in an ABCP program and also provides pool-specific liquidity facilities that cover 100 percent of each of the underlying asset pools. The bank would be required to hold capital against 10 percent of the underlying asset pools because it is providing the program-wide credit enhancement. The bank would also be required to hold capital against 90 percent of the liquidity facilities it is providing to each of the underlying asset pools. For risk-based capital purposes, the bank would not be required to hold capital against any credit enhancements or liq-

17. See the Board staff's October 12, 2007, legal interpretation regarding the risk-based capital treatment of ABCP liquidity facilities.

quidity facilities that comprise the same program assets.

If different banks have overlapping exposures to an ABCP program, however, each organization must hold capital against the entire maximum amount of its exposure. As a result, while duplication of capital charges will not occur for individual banks, some systemic duplication may occur where multiple BOs have overlapping exposures to the same ABCP program.

Asset-quality test. For a liquidity facility, either short- or long-term, that supports ABCP *not* to be considered a recourse obligation or a direct-credit substitute, it must meet the risk-based capital rule's definition of an *eligible ABCP liquidity facility.* An eligible ABCP liquidity facility must meet a reasonable asset-quality test that, among other things, precludes funding against assets that are 90 days or more past due or in default. When assets are 90 days or more past due, they typically have deteriorated to the point where there is an extremely high probability of default. Assets that are 90 days past due, for example, often must be placed on nonaccrual status in accordance with the agencies' Uniform Retail Credit Classification and Account Management Policy.[18] Further, they generally must also be classified substandard under that policy.

In addition to the above, if the assets covered by the liquidity facility are initially externally rated (at the time the facility is provided), the facility can be used to fund only those assets that are externally rated investment grade at the time of funding. The practice of purchasing assets that are externally rated below investment grade out of an ABCP program is considered to be the equivalent of providing credit protection to the commercial paper investors. Thus, liquidity facilities permitting purchases of below-investment-grade securities will be considered either recourse obligations or direct-credit substitutes.

However, neither the "90-days-past-due" limitation nor the "investment grade" limitation apply to the asset-quality test with respect to assets that are conditionally or unconditionally guaranteed by the U.S. government or its agencies or by another OECD central government.

An ABCP liquidity facility is considered to be in compliance with the requirement for an asset quality test if (1) the liquidity provider has access to certain types of acceptable credit enhancements and (2) the notional amount of such credit enhancements available to the liquidity facility provider exceeds the amount of underlying assets that are 90 days or more past due, defaulted, or below investment grade for which the liquidity provider may be obligated to fund under the facility. In this circumstance, the liquidity facility may be considered "eligible" for purposes of the risk-based capital rule because the provider of the credit enhancement generally bears the credit risk of the assets that are 90 days or more past due, in default, or below investment grade rather than the banking organization providing liquidity.[19]

The following forms of credit enhancements are generally acceptable for purposes of satisfying the asset quality test:

- "funded" credit enhancements that the BO may access to cover delinquent, defaulted, or below-investment-grade assets, such as overcollateralization, cash reserves, subordinated securities, and funded spread accounts;
- surety bonds and letters of credit issued by a third party with a nationally recognized statistical rating organization with a rating of single A or higher that the BO may access to cover delinquent, defaulted, or below-investment-grade assets, provided that the surety bond or letter of credit is irrevocable and legally enforceable; and
- one month's worth of excess spread that the BO may access to cover delinquent, defaulted, or below-investment-grade assets if the following conditions are met: (1) excess spread is contractually required to be trapped when it falls below 4.5 percent (measured on an annualized basis) and (2) there is no material adverse change in the BO's ABCP underwriting standards. The amount of available excess spread may be calculated as the average of the current month's and the two previous months' excess spread.

Recourse directly to the seller, other than the funded credit enhancements enumerated above, regardless of the seller's external credit rating, is not an acceptable form of credit enhancement

18. See 65 *Fed. Reg.* 36904 (June 12, 2000).

19. See SR-05-13 and its attachment, "Interagency Guidance on the Eligibility of Asset-Backed Commercial Paper Liquidity Facilities and the Resulting Risk-Based Capital Treatment."

for purposes of satisfying the asset quality test. Seller recourse—for example, a seller's agreement to buy back nonperforming or defaulted loans or downgraded securities—may expose the liquidity provider to an increased level of credit risk. A decline in the performance of assets sold to an ABCP conduit may signal impending difficulties for the seller.

If the amount of acceptable credit enhancement associated with the pool of assets is less than the current amount of assets that are 90 days or more past due, in default, or below investment grade that the liquidity facility provider may be obligated to fund against, the liquidity facility should be treated as recourse or a direct credit substitute. The full amount of assets supported by the liquidity facility would be subject to a 100 percent credit conversion factor.[19a] The Federal Reserve Board reserves the right to deem an otherwise eligible liquidity facility to be, in substance, a direct credit substitute if a member bank uses the liquidity facility to provide credit support.

The bank is responsible for demonstrating to the Federal Reserve Board whether acceptable credit enhancements cover the 90 days or more past due, defaulted, or below-investment-grade assets that the organization may be obligated to fund against in each seller's asset pool. If the bank cannot adequately demonstrate satisfaction of the conditions in the above-referenced interagency guidance, the Federal Reserve Board further reserves the right to determine that a credit enhancement is unacceptable for purposes of the requirement for an asset quality test and, therefore, it may deem the liquidity facility to be ineligible.

Market risk capital requirements for ABCP programs. Any facility held in the trading book whose primary function, in form or in substance, is to provide liquidity to ABCP—even if the facility does not qualify as an eligible ABCP liquidity facility under the rule—will be subject to the banking-book risk-based capital requirements. Specifically, banks are required to convert the notional amount of all trading-book positions that provide liquidity to ABCP to credit-equivalent amounts by applying the appropriate banking-book credit-conversion factors. For example, the full amount of all eligible ABCP liquidity facilities with an original maturity of one year or less will be subject to a 10 percent conversion factor, regardless of whether the facility is carried in the trading account or the banking book.

19a. See 12 CFR 208, appendix A, section III.B.3.b.i.

SOUND RISK-MANAGEMENT PRACTICES

An institution must incorporate the risks involved in its securitization activities into its overall risk-management system. The system should entail (1) inclusion of risk exposures in reports to the institution's senior management and board to ensure proper management oversight; (2) adoption of appropriate policies, procedures, and guidelines to manage the risks involved; (3) appropriate measurement and monitoring of risks; and (4) assurance of appropriate internal controls to verify the integrity of the management process with respect to these activities.

Board and Senior Management Oversight

Both the board of directors and senior management are responsible for ensuring that they fully understand the degree to which the organization is exposed to the credit, market, liquidity, operational, legal, and reputational risks involved in the institution's securitization activities. They are also responsible for ensuring that the formality and sophistication of the techniques used to manage these risks are commensurate with the nature and volume of the organization's activities. Institutions with significant securitization activities are expected to have more elaborate and formal approaches to manage the risk of these activities. The board should approve all significant policies relating to the management of risk arising from securitization activities and should ensure that risk exposures are fully incorporated in board reports and risk-management reviews.

Policies and Procedures

Senior management is responsible for ensuring that the risks arising from securitization activities are adequately managed on both a short-term and long-run basis. Management should

ensure that adequate policies and procedures are in place for incorporating the risk of these activities into the overall risk-management process of the institution. Such policies should ensure that the economic substance of the risk exposures generated by these activities is fully recognized and appropriately managed. In addition, BOs involved in securitization activities should have appropriate policies, procedures, and controls for underwriting ABS; funding the possible return of revolving receivables (for example, credit card receivables and home-equity lines); and establishing limits on exposures to individual institutions, types of collateral, and geographic and industrial concentrations. The institution's directors and managers need to ensure that—

- independent risk-management processes are in place to monitor securitization-pool performance on an individual and aggregate transaction level (an effective risk-management function includes appropriate information systems to monitor securitization activities);
- conservative valuation assumptions and modeling methodologies are used to establish, evaluate, and adjust the carrying value of retained interests on a regular and timely basis;
- audit or internal-review staffs periodically review data integrity, model algorithms, key underlying assumptions, and the appropriateness of the valuation and modeling process for the securitized assets the institution retains (the findings of such reviews should be reported directly to the board or an appropriate board committee);
- accurate and timely risk-based capital calculations are maintained, including recognition and reporting of any recourse obligation resulting from securitization activity;
- internal limits are in place to govern the maximum amount of retained interests as a percentage of total equity capital; and
- the institution has a realistic liquidity plan in place in case of market disruptions.

Independent Risk-Management Function

Institutions engaged in securitizations need to have an independent risk-management function commensurate with the complexity and volume of their securitizations and their overall risk exposures. The risk-management function should ensure that securitization policies and operating procedures, including clearly articulated risk limits, are in place and appropriate for the institution's circumstances. A sound asset-

securitization policy should include or address, at a minimum—

- a written and consistently applied accounting methodology;
- regulatory reporting requirements;
- valuation methods, including FAS 140 residual-value assumptions, and procedures to formally approve changes to those assumptions;
- a management reporting process; and
- exposure limits and requirements for both individual- and aggregate-transaction monitoring.

It is essential that the risk-management function monitor origination, collection, and default-management practices. This includes regular evaluations of the quality of underwriting, soundness of the appraisal process, effectiveness of collections activities, ability of the default-management staff to resolve severely delinquent loans in a timely and efficient manner, and appropriateness of loss-recognition practices. Because the securitization of assets can result in the current recognition of anticipated income, the risk-management function should pay particular attention to the types, volumes, and risks of assets being originated, transferred, and serviced. Senior management and the risk-management staff must be alert to any pressures on line managers to originate abnormally large volumes or higher-risk assets to sustain ongoing income needs. Such pressures can lead to a compromise of credit-underwriting standards. This may accelerate credit losses in future periods, impair the value of retained interests, and potentially lead to funding problems.

Risk Measurement and Monitoring

An institution's risk-management function should include information and risk-measurement and -monitoring systems that fully incorporate the risks involved in its securitization activities. BOs must be able to identify credit exposures from all securitization activities, as well as measure, quantify, and control those exposures on a fully consolidated basis. The economic substance of the credit exposures of securitization activities should be fully incorporated into the institution's efforts to quantify its credit risk, including efforts to establish more formal grading of credits to allow for statistical estimation of loss-probability distributions. Securitization activities should also be included in any aggregations of credit risk by borrower, industry, or economic sector.

An institution's information systems should identify and segregate those credit exposures arising from the institution's loan-sale and securitization activities. Such exposures include the sold portions of participations and syndications, exposures arising from the extension of credit-enhancement and liquidity facilities, the effects of an early-amortization event, and the investment in ABS. The management reports should provide the board and senior management with timely and sufficient information to monitor the institution's exposure limits and overall risk profile.

Stress Testing

The use of stress testing, including combinations of market events that could affect a BO's credit exposures and securitization activities, is another important element of risk management. Stress testing involves identifying possible events or changes in market behavior that could have unfavorable effects on the institution, and assessing the organization's ability to withstand them. Stress testing should consider not only the probability of adverse events but also likely worst-case scenarios. Stress testing should be done on a consolidated basis and should consider, for instance, the effect of higher-than-expected levels of delinquencies and defaults, as well as the consequences of early-amortization events with respect to credit card securities, that could raise concerns regarding the institution's capital adequacy and its liquidity and funding capabilities. Stress-test analyses should also include contingency plans for possible management actions in certain situations.

Internal Controls

One of management's most important responsibilities is establishing and maintaining an effective system of internal controls. Among other things, internal controls should enforce the official lines of authority and the appropriate separation of duties in managing the risks of the institution. These internal controls must be suitable for the type and level of risks at the institution, given the nature and scope of its

activities. Moreover, these internal controls should ensure that financial reporting is reliable (in published financial reports and regulatory reports), including adequate allowances or liabilities for expected losses.

Effective internal controls are essential to an institution's management of the risks associated with securitization. When properly designed and consistently enforced, a sound system of internal controls will help management safeguard the institution's resources; ensure that financial information and reports are reliable; and comply with contractual obligations, including securitization covenants. Internal controls will also reduce the possibility of significant errors and irregularities, and assist in their timely detection. Internal controls typically (1) limit authorities; (2) safeguard access to and use of records; (3) separate and rotate duties; and (4) ensure both regular and unscheduled reviews, including testing.

Operational and managerial standards have been established for internal control and information systems.[20] A system of internal controls should be maintained that is appropriate to the institution's size and nature, its scope, and the risk of its activities.[21]

Audit Function or Internal Review

The institution's board of directors is responsible for ensuring that its audit staff or independent-review function is competent to review its securitization activities. The audit function should perform periodic reviews of securitization activities, including transaction testing and verification, and report all findings to the board or appropriate board committee. The audit function also may be useful to senior management in identifying and measuring risk related to securitization activities. Principal audit targets should include compliance with securitization policies, operating and accounting procedures (FAS 140), deal covenants, and the accuracy of MIS and regulatory reports. The audit function also should confirm that the institution's regulatory reporting process is designed and managed to facilitate timely and accurate report filing. Furthermore, when a third party services loans, the auditors should perform an independent verification of the existence of the loans to ensure that balances reconcile to internal records.

Management Information Systems

An institution's reporting and documentation methods must support the initial valuation of any retained interests and provide ongoing impairment analyses of these assets. Pool-performance information will help well-managed institutions ensure, on a qualitative basis, that a sufficient amount of economic capital is being held to cover the various risks inherent in securitization transactions. The absence of an adequate management information system (MIS) will hinder management's ability to monitor specific pool performance and securitization activities. MIS reports, at a minimum, should address the following:

- *Securitization summaries for each transaction.* The summary should include relevant transaction terms such as collateral type, facility amount, maturity, credit-enhancement and subordination features, financial covenants (termination events and spread-account capture "triggers"), right of repurchase, and counterparty exposures. Management should ensure that the summaries for each transaction are distributed to all personnel associated with securitization activities.
- *Performance reports by portfolio and specific product type.* Performance factors include gross portfolio yield, default rates and loss severity, delinquencies, prepayments or payments, and excess spread amounts. The reports should reflect the performance of assets, both on an individual-pool basis and total managed assets. These reports should segregate specific products and different marketing campaigns.
- *Vintage analysis for each pool using monthly data.* Vintage analysis will help management understand historical performance trends and their implications for future default rates, prepayments, and delinquencies, and therefore retained interest values. Management can use

20. See the safety-and-soundness standards for national banks at 12 CFR 30 (OCC) and for savings associations at 12 CFR 570 (OTS).

21. Institutions that are subject to the requirements of FDIC regulation 12 CFR 363 should include an assessment of the effectiveness of internal controls over their asset-securitization activities as part of management's report on the overall effectiveness of the system of internal controls over financial reporting. This assessment implicitly includes the internal controls over financial information that is included in regulatory reports.

these reports to compare historical performance trends with underwriting standards, including the use of a validated credit-scoring model, to ensure loan pricing is consistent with risk levels. Vintage analysis also helps in the comparison of deal performance at periodic intervals and validates retained-interest valuation assumptions.

- *Static-pool cash-collection analysis.* A static-pool cash-collection analysis involves reviewing monthly cash receipts relative to the principal balance of the pool to determine the cash yield on the portfolio, comparing the cash yield to the accrual yield, and tracking monthly changes. Management should compare monthly the timing and amount of cash flows received from the trust with those projected as part of the FAS 140 retained-interest valuation analysis. Some master-trust structures allow excess cash flow to be shared between series or pools. For revolving-asset trusts with this master-trust structure, management should perform a cash-collection analysis for each master-trust structure. These analyses are essential in assessing the actual performance of the portfolio in terms of default and prepayment rates. If cash receipts are less than those assumed in the original valuation of the retained interest, this analysis will provide management and the board with an early warning of possible problems with collections or extension practices and impairment of the retained interest.
- *Sensitivity analysis.* A sensitivity analysis measures the effect of changes in default rates, prepayment or payment rates, and discount rates to assist management in establishing and validating the carrying value of the retained interest. Stress tests should be performed at least quarterly. Analyses should consider potential adverse trends and determine "best," "probable," and "worst-case" scenarios for each event. Other factors that need to be considered are the impact of increased defaults on collections staffing, the timing of cash flows, spread-account capture triggers, overcollateralization triggers, and early-amortization triggers. An increase in defaults can result in higher-than-expected costs and a delay in cash flows, thus decreasing the value of the retained interests. Management should periodically quantify and document the potential impact to both earnings and capital and should report the results to the board of directors. Management should incorporate this analysis into their overall interest-rate risk measurement system.[22] Examiners will review the institution's analysis and the volatility associated with retained interests when assessing the Sensitivity to Market Risk component rating (the "S" in the CAMELS rating system for banks or the "R" for the BHC RFI/C(D) rating system).[23]
- *Statement of covenant compliance.* Ongoing compliance with deal-performance triggers as defined by the pooling and servicing agreements should be affirmed at least monthly. Performance triggers include early amortization, spread capture, changes to overcollateralization requirements, and events that would result in servicer removal.

Securitization Convenants Linked to Supervisory Actions or Thresholds

A bank's board of directors and senior management are responsible for initiating policies and procedures and for monitoring processes and internal controls that will provide reasonable assurance that the bank's contracts and commitments do not include detrimental covenants that affect the safety and soundness of the bank. When examiners review a bank's securitization contracts and related documentation, they should be alert to any covenants that use adverse supervisory actions or the breach of supervisory thresholds as triggers for early-amortization events or the transfer of servicing. Examples of such supervisory actions include a downgrade in the organization's CAMELS rating, an enforcement action, or a downgrade in a bank's prompt-corrective-action capital category. The inclusion of supervisory-linked covenants in securitization documents is considered to be an "unsafe and unsound banking practice" that undermines the objective of supervisory actions and thresholds. An early amortization or transfer of servicing triggered by such events can create or exacerbate liquidity and earnings problems for a bank that may lead to further deterioration in its financial condition.

22. The Joint Agency Policy Statement on Interest-Rate Risk (see SR-96-13 and section 4090.1) advises institutions with a high level of exposure to interest-rate risk relative to capital that they will be directed to take corrective action.

23. See the appendix to section 5020.1 (section A.5020.1) for a description of the CAMELS rating system. See SR-04-18 for a description of the RFI/C(D) rating system.

Convenants that contain triggers tied, directly or indirectly, to supervisory actions or thresholds can also result in the early amortization of a securitization at a time when the sponsoring organization's ability to access other funding sources is limited. If an early-amortization event occurs, investors may lose confidence in the stability of the sponsoring organization's asset-backed securities, thus limiting its ability to raise new funds through securitization. At the same time, the organization must fund new receivables on the balance sheet, potentially resulting in liquidity problems. Moreover, the existence of a supervisory-linked trigger potentially could inhibit supervisors from taking action intended to address problems at a troubled institution because the action could trigger an event that worsens the institution's condition or causes its failure.

The Federal Reserve and the other federal banking agencies (the OCC, the FDIC, and the OTS) also are concerned that covenants related to supervisory actions may obligate a bank's management to disclose confidential examination information, such as the CAMELS rating. Disclosure of such information by a bank's directors, officers, employees, attorneys, auditors, or independent auditors, without explicit authorization by the institution's primary regulator, violates the agencies' information-disclosure rules and may result in follow-up supervisory actions. (See SR-02-14.)

Because of the supervisory concerns about convenants linked to supervisory actions, a federal bank interagency advisory was issued on May 23, 2002. The advisory emphasizes that a bank's management and board of directors should ensure that covenants related to supervisory actions or thresholds are not included in securitization documents. Covenants that provide for the early termination of the transaction or compel the transfer of servicing due, directly or indirectly, to the occurrence of a supervisory action or event will be criticized, under appropriate circumstances, as an unsafe and unsound banking practice. The agencies also may take other supervisory actions, such as requiring additional capital or denying capital relief for risk-based capital calculations, regardless of the GAAP treatment.

Examiners should consider the potential impact of such covenants in existing transactions when evaluating both the overall condition of the bank and the specific component ratings of capital, liquidity, and management. Early-amortization triggers will specifically be considered in the context of the bank's overall liquidity position and contingency funding plan. For organizations with limited access to other funding sources or a significant reliance on securitization, the existence of these triggers presents a greater degree of supervisory concern. Any bank that uses securitization as a funding source should have a viable contingency funding plan in the event it can no longer access the securitization market. Examiners should encourage bank management to amend, modify, or remove covenants linked to supervisory actions from existing transactions. Any impediments a bank may have to taking such actions should be documented and discussed with the appropriate supervisory staff of its responsible Reserve Bank.

APPRAISALS AND MORTGAGE-BACKED SECURITIES

Under 12 CFR 225.63(a)(8), an appraisal performed by a state-certified or -licensed appraiser is not required for any real estate–related financial transaction in which a regulated institution purchases a loan or interest in a loan; pooled loans; or an interest in real property, including mortgage-backed securities, provided that the appraisal prepared for each pooled loan or real property interest met the requirements of the regulation. Banks must establish procedures for determining and ensuring that applicable appraisals meet the requirements.

EXAMINATION GUIDELINES FOR ASSET SECURITIZATION

A banking organization may be involved in originating the assets to be pooled, packaging the assets for securitization, servicing the pooled assets, acting as trustee for the pool, providing credit enhancements, underwriting or placing the ABS, or investing in the securities. Individual securitization arrangements often possess unique features, and the risks addressed in this abbreviated version of the examiner guidelines[24]

24. A complete version of the "Examination Guidelines for Asset Securitization" is attached to SR-90-16.

do not apply to all securitization arrangements. Conversely, arrangements may entail risks not summarized here. Examiners should judge a banking organization's exposure to securitization with reference to the specific structures in which the organization is involved and the degree to which the organization has identified exposures and implemented policies and controls to manage them. Examiners may tailor the scope of their examinations if the banking organization's involvement in securitization is immaterial relative to its size and financial strength.

A banking organization participating in securitization, in any capacity, should ensure that the activities are clearly and logically integrated into the overall strategic objectives of the organization. The management of the organization should understand the risks and should not rely excessively on outside expertise to make crucial decisions regarding securitization activities.

As mentioned earlier, the degree of securitization exposure faced by an individual banking organization depends on the role of the organization in the securitization process. An organization involved in the issuance of ABS as originator, packager, servicer, credit enhancer, underwriter, or trustee may face combinations and degrees of risk different than those faced by an organization that only invests in ABS. Examiners should assess a BO's level, identification, and management of risks within the context of its roles.

A BO should conduct an independent analysis of its exposures before participating in any aspect of securitization and should continue to monitor its exposures throughout its involvement. The analysis and subsequent monitoring should take into account the entire securitization arrangement, emphasizing different risks according to the role that the organization plays. Excessive reliance on opinions of third parties and reported collateral values should be avoided.

An organization involved in the issuance of ABS should scrutinize the underlying assets, giving consideration to their yield, their maturity, their credit risk, their prepayment risk, and the accessibility of collateral in cases of default, as well as the structure of the securitization arrangement and the ability of the other participants in the transaction to meet their obligations. On the other hand, a BO investing in ABS can be expected to place greater emphasis on the characteristics of the ABS as securities, paying attention primarily to credit risk, prepayment risk, liquidity risk, and concentration risk; the underlying assets and structure of the securitization arrangement would be evaluated only within this context.

Appropriate policies, procedures, and controls should be established by a BO before participating in asset securitization. Controls should include well-developed management information systems. In addition, significant policies and procedures should be approved and reviewed periodically by the organization's board of directors.

In addition to evaluating and monitoring exposure to particular securitization deals, a BO should manage its overall exposure on a consolidated holding company basis. Management of these exposures should include—

- reasonable limits on geographic and industrial concentrations, as well as on exposures to individual institutions;
- internal systems and controls to monitor these exposures and provide periodic and timely reports to senior management and the board of directors on performance and risks; and
- procedures for identifying potential or actual conflicts of interest and policies for resolving those conflicts.

The following general guidelines are intended to help examiners assess the exposures of banks and bank holding companies to asset securitization.

Banking Organizations Involved in Issuing or Managing ABS

A BO involved in the issuance of ABS as originator, packager, servicer, credit enhancer, underwriter, or trustee should analyze the assets underlying the asset-backed security and the structure of the arrangement, including—

- the characteristics and expected performance of the underlying assets,
- the BO's ability to meet its obligations under the securitization arrangement, and
- the ability of the other participants in the arrangement to meet their obligations.

Analysis of the underlying assets should be conducted independently by each participant in the process, giving consideration to yield,

maturity, credit risk, prepayment risk, and the accessibility of collateral in cases of default. An originator should further consider the impact of securitization on the remaining asset portfolio and on the adequacy of loan-loss reserves and overall capital.

Financial position and operational capacity should be adequate to meet obligations to other parties in a securitization arrangement, even under adverse scenarios. Accordingly, a BO should ensure that the pricing of services is adequate to cover costs over the term of the obligation, as well as to compensate for associated risks. Further, the organization should have contingency plans to transfer responsibilities to another institution in the event that those responsibilities can no longer be fulfilled. Examiners should determine that the BO has policies and controls for managing contractual obligations, including management of collateral, if applicable. Staffing levels should be adequate to fulfill responsibilities.

If a BO's obligations, under a securitization agreement, are subcontracted to other parties, an assessment of the subcontractor's financial position and operational capacity should be conducted before delegating responsibility. Further, the subcontractor's financial position and compliance with contractual obligations should be monitored periodically.

A BO involved in issuing ABS should make certain that the agreement permits it to assess the ability of other participants in the securitization arrangement to meet their obligations (considering obligations that they may have under other securitization arrangements). The rights and obligations of each of the participants under possibly novel legal and institutional arrangements should be clearly documented.

Funding and liquidity management for originators and packagers of securitized assets should avoid excessive reliance on the device of securitization. Originators and packagers should monitor the securitization market closely, develop a broad customer base for their securitization activities, and maintain diversified funding sources.

BOs should not rely excessively on the expertise of a single individual or a small group of individuals, either inside or outside the organization, for the management of participation in securitization activities. Examiners should ensure that an organization acting as trustee for ABS follows the usual standards for trust services.

Policy and Portfolio Analysis

Credit risk. Institutions should be aware that the credit risk involved in many securitization activities may not always be obvious. For certain types of loan-sales and securitization transactions, a BO may actually be exposed to essentially the same credit risk as in traditional lending activities, even though a particular transaction may, superficially, appear to have isolated the institution from any risk exposure. In such cases, removal of an asset from the balance sheet may not result in a commensurate reduction in credit risk. Transactions that can give rise to such instances include loan sales with recourse; credit derivatives; direct-credit substitutes, such as letters of credit; and liquidity facilities extended to securitization programs, as well as certain asset-securitization structures, such as the structure typically used to securitize credit card receivables.

The partial, first-loss recourse obligations an institution retains when selling assets, and the extension of partial credit enhancements (for example, 10 percent letters of credit) in connection with asset securitization, can be sources of concentrated credit risk by exposing institutions to the full amount of expected losses on the protected assets. For instance, the credit risk associated with whole loans or pools of assets that are sold to secondary-market investors can often be concentrated within the partial, first-loss recourse obligations retained by the BOs that are selling and securitizing the assets. In these situations, even though institutions may have reduced their exposure to catastrophic loss on the assets sold, they generally retain the same credit-risk exposure that they would have had if they continued to hold the assets on their balance sheets.

In addition to recourse obligations, institutions assume concentrated credit risk through the extension of partial direct-credit substitutes, such as through the purchase (or retention) of subordinated interests in their own asset securitizations or through the extension of letters of credit. For example, BOs that sponsor certain asset-backed commercial paper programs, or so-called remote-origination conduits, can be exposed to high degrees of credit risk even though it may seem that their notional exposure is minimal. A remote-origination conduit lends directly to corporate customers referred to it by the sponsoring BO that used to lend directly to these same borrowers. The conduit funds this

lending activity by issuing commercial paper that, in turn, is guaranteed by the sponsoring BO. The net result is that the sponsoring institution has much the same credit-risk exposure through this guarantee that it would have had if it had made the loans directly and held them on its books. This is an off-balance-sheet transaction, however, and its associated risks may not be fully reflected in the institution's risk-management system.

Furthermore, BOs that extend liquidity facilities to securitized transactions, particularly to asset-backed commercial paper programs, may be exposed to high degrees of credit risk which may be subtly embedded within a facility's provisions. Liquidity facilities are commitments to extend short-term credit to cover temporary shortfalls in cash flow. While all commitments embody some degree of credit risk, certain commitments extended to asset-backed commercial paper programs to provide liquidity may subject the extending institution to the credit risk of the underlying asset pool, often trade receivables, or of a specific company using the program for funding. Often, the stated purpose of these liquidity facilities is to provide funds to the program to retire maturing commercial paper when a mismatch occurs in the maturities of the underlying receivables and the commercial paper, or when a disruption occurs in the commercial paper market. However, depending on the provisions of the facility—such as whether the facility covers dilution of the underlying receivable pool—credit risk can be shifted from the program's explicit credit enhancements to the liquidity facility.[25] Such provisions may enable certain programs to fund riskier assets and yet maintain the credit rating on the program's commercial paper without increasing the program's credit-enhancement levels.

The structure of various securitization transactions can also result in an institution's retaining the underlying credit risk in a sold pool of assets. Examples of this contingent credit-risk retention include credit card securitizations in which the securitizing organization explicitly sells the credit card receivables to a master trust, but, in substance, retains the majority of the economic risk of loss associated with the assets because of the credit protection provided to investors by the excess yield, spread accounts, and structural provisions of the securitization. Excess yield provides the first level of credit protection that can be drawn upon to cover cash shortfalls between the principal and coupon owed to investors and the investors' pro rata share of the master trust's net cash flows. The excess yield is equal to the difference between the overall yield on the underlying credit card portfolio and the master trust's operating expenses.[26] The second level of credit protection is provided by the spread account, which is essentially a reserve funded initially from the excess yield.

In addition, the structural provisions of credit card securitizations generally provide credit protection to investors through the triggering of early-amortization events. Such an event usually is triggered when the underlying pool of credit card receivables deteriorates beyond a certain point and requires that the outstanding credit card securities begin amortizing early to pay off investors before the prior credit enhancements are exhausted. As the early amortization accelerates the redemption of principal (paydown) on the security, the credit card accounts that were assigned to the master credit-card trust return to the securitizing institution more quickly than had originally been anticipated. Thus, the institution is exposed to liquidity pressures and any further credit losses on the returned accounts.

Examiner procedures for reviewing credit risk are outlined below:

- Examiners should review a BO's policies and procedures to ensure that the organization follows prudent standards of credit assessment and approval for all securitization exposure. Procedures should include an initial thorough and independent credit assessment of each loan or pool for which it has assumed credit risk, followed by periodic credit reviews to monitor performance throughout the life of the exposure.
- Examiners should determine that rigorous credit standards are applied, regardless of the role an organization plays in the issuance of ABS. The servicer, credit enhancer, and under-

25. Dilution essentially occurs when the receivables in the underlying asset pool—before collection—are no longer viable financial obligations of the customer. For example, dilution can arise from returns of consumer goods or unsold merchandise by retailers to manufacturers or distributors.

26. The monthly excess yield is the difference between the overall yield on the underlying credit card portfolio and the master trust's operating expenses. It is calculated by subtracting from the gross portfolio yield (1) the coupon paid to investors; (2) charge-offs for that month; and (3) a servicing fee, usually 200 basis points, paid to the banking organization sponsoring the securitization.

writer must perform assessments and approvals independent of and distinct from reviews provided by the originator or packager.
- Major policies and procedures, including internal credit-review and -approval procedures and in-house exposure limits, should be reviewed periodically and approved by the institution's board of directors.
- Failure, fraud, or mismanagement on the part of one participant in an ABS issue could result in loss to any of the other institutions involved in the issue. A BO involved in securitization should have adequate procedures for evaluating the internal control procedures and financial strength of other institutions with which it is involved.
- Securitization arrangements may remove a credit enhancer from direct access to the collateral. The remedies available to a BO involved in the provision of credit enhancement in the event of a default should be clearly documented.
- Examiners should ensure that, regardless of the role an institution plays in securitization, ABS documentation clearly specifies the limitations of the institution's legal responsibility to assume losses.
- Examiners should verify that a banking organization acting as originator, packager, or underwriter has written policies addressing the repurchase of assets and other reimbursement to investors in the event that a defaulted package results in losses exceeding any contractual credit enhancement. A BO that repurchases defaulted assets or pools in contradiction of the underlying agreement in effect sets a standard by which it could potentially be found legally liable for all ''sold'' assets. A BO that responds in this manner to the ''moral hazard'' or reputational risk arising from its securitization activities may face additional risk from other areas of its securitization activities. Examiners should review any situations in which the organization has repurchased or otherwise reimbursed investors for poor-quality assets.
- A BO's records should be reviewed to ensure that credit, pricing, and servicing standards for securitized assets are equivalent to standards for assets that remain on the books. The quality of securitized assets should be accurately characterized to investors and other parties to the securitization arrangement to avoid unforeseen pressures to repurchase defaulted issues.
- Pricing policies and practices should be reviewed to determine that they incorporate an analysis of the tradeoff between risk and return.
- Examiners should consider securitization risks when analyzing the adequacy of an organization's capital or reserve levels. Adverse credit risk should be classified accordingly.

Concentration risk. A banking organization involved in originating, packaging, servicing, underwriting, or enhancing the creditworthiness of ABS must take special care to follow in-house diversification requirements for aggregate outstandings to a particular institution, industry, or geographic area. Examiner procedures for reviewing concentration risk are outlined below:

- When determining compliance with internal credit-exposure limits, securitization exposure should be aggregated with all loans, extensions of credit, debt and equity securities, legally binding financial guarantees, commitments, and any other investments involving the same obligor.
- Examiners should review all pools of sold assets for industrial or geographic concentrations. Excessive exposures to an industry or region among these assets should be noted in the review of the BO's loan portfolio.
- Inherent in securitization is the risk that, if another party involved in the securitization arrangement becomes unable to perform according to contract terms, the issue might default even while the underlying credits are performing. This credit exposure to the other managing parties in a securitization transaction should be included under a BO's general line to those institutions. Examiners should, therefore, ensure that, in addition to policies limiting direct credit exposure, an institution has developed exposure limits with respect to particular originators, credit enhancers, and servicers.

Reputational risk. The securitization activities of many institutions may also expose them to significant reputational risks. Often, BOs that sponsor the issuance of asset-backed securities act as servicers, administrators, or liquidity providers in the securitization transactions. These institutions must be aware of the potential losses and risk exposure associated with reputational risk that arise from these securitization activities. The securitization of assets whose perfor-

mance has deteriorated may result in a negative market reaction that could increase the spreads on an institution's subsequent issuances. To avoid a possible increase in their funding costs, institutions have supported their securitization transactions by improving the performance of the securitized asset pool (for example, by selling discounted receivables or adding higher-quality assets to the securitized asset pool). Thus, an institution's voluntary support of its securitization in order to protect its reputation can adversely affect the sponsoring or issuing organization's earnings and capital.

Liquidity and market risk. The existence of recourse provisions in asset sales, the extension of liquidity facilities to securitization programs, and early-amortization triggers of certain asset-securitization transactions can involve significant liquidity risk to institutions engaged in these securitization activities. Institutions should ensure that their liquidity contingency plans fully incorporate the potential risk posed by their securitization activities. When new ABS are issued, the issuing banking organization should determine their potential effect on its liquidity at the inception of each transaction and throughout the life of the securities to better ascertain its future funding needs.

An institution's contingency plans should consider the need to obtain replacement funding and specify the possible alternative funding sources, in the event of the amortization of outstanding ABS. Replacement funding is particularly important for securitizations of revolving receivables, such as credit cards, in which an early amortization of the ABS could unexpectedly return the outstanding balances of the securitized accounts to the issuing institution's balance sheet. Early amortization of a banking organization's ABS could impede an institution's ability to fund itself—either through reissuance or other borrowings—since the institution's reputation with investors and lenders may be adversely affected. Moreover, the liquidity risk and market risk to which ABS are subject may be exacerbated by thin secondary markets for them. Examiner procedures for reviewing liquidity and market risk are outlined below:

- Examiners should review the policies of a BO engaged in underwriting, looking for situations in which it cannot sell underwritten ABS. Credit review, funding capabilities, and approval limits should allow the institution to purchase and hold unsold securities. In the absence of this analysis, the institution should only handle ABS on a best-efforts basis. All potential credit exposure should be within legal lending limits.
- Examiners should ensure that a BO engaged in underwriting or market making has implemented adequate hedging or other risk-management policies to limit its exposure to adverse price movements.
- Examiners should determine whether an organization targets certain loans at origination to be packaged and securitized. If so, examiners should review the length of time these assets are held while being processed. Examiners should review management information systems reports to age targeted loans and to determine if there is any decline in value while the loans are in the pipeline. Loans held for resale in this pipeline should be segregated and carried at the lower of cost or market value.

Transfer risk and operational risk. Transfer risk is analogous to liquidity risk. It is the risk that an organization with obligations under securitization arrangements may wish to relinquish those obligations but may not be able to do so. Operational risk arises from uncertainty about an organization's ability to meet its obligations under securitization arrangements and may arise from insufficient computer resources or from a failure of fees to cover associated costs. An organization filling a role that potentially requires long-term resource commitments, such as servicer or credit enhancer, is most susceptible to transfer risk and operational risk. Examiner procedures for reviewing transfer and operational risk are outlined below:

- Examiners should determine that a BO has reviewed the relevant contracts to verify that they are free of any unusual features that increase the potential cost of transfer of obligations.
- Examiners should ascertain that a BO has evaluated the fee structure of the securitization to determine that fees are sufficient to cover the costs of associated services. Further, examiners should determine that a BO has reviewed the projected cash flow from the underlying assets to ensure that principal and interest payments will be timely and will be sufficient to cover costs, even under adverse scenarios.

- A servicer or credit enhancer subcontracting or participating responsibilities should initially assess the financial condition and reputation of any organization to which responsibility may be delegated. Subsequent periodic monitoring by the servicer or credit enhancer should assess the financial condition of organizations to which responsibility has been delegated, as well as their compliance with contractual obligations. Trustees should, likewise, monitor the financial condition and compliance of all participants in the securitization arrangement.

Conflicts of interest. With respect to the various functions performed by a BO, the potential for conflicts of interest exists when an organization plays multiple roles in securitization. Policies and procedures must address this potential conflict, especially the risk of legal ramifications or negative market perceptions if the organization appears to compromise its fiduciary responsibility to obligors or investors. Examiner procedures for reviewing conflicts of interest are outlined below:

- Examiners should review a BO's policies for disclosure of confidential but pertinent information about the underlying assets and obligors. An organization involved in the origination or processing of a securitization transaction should have written statements from obligors allowing the disclosure of pertinent confidential information to potential investors. In addition, the underwriting bank must follow proper procedures of due diligence.
- If the securitization business of an originator, underwriter, or credit enhancer is volume-driven, legal obligations or prudent banking practices may be breached. Examiners should review credit standards used in analyzing assets earmarked for securitization to determine that sound banking practices are not being compromised to increase volume or to realize substantial fees.
- Examiners should determine that the organization's policies addressing activities at various subsidiaries or affiliates are managed consistently and prudently in compliance with regulatory policies.

Legal Review and Liability

The complexity of asset-securitization transactions requires a BO that participates in them in any capacity to fully investigate all applicable laws and regulations, to establish policies and procedures to ensure legal review of all securitization activities, and to take steps to protect the organization from liability in the case of problems with particular asset-backed issues. Organizations and examiners should be aware of the continual evolution of criteria on the types of assets that may be securitized and the types of BOs that may engage in the various aspects of securitization. Examiner procedures for checking an institution's legal-review and liability-protection measures are outlined below:

- Different responsibilities in connection with securitizations may be split among various subsidiaries of an organization. Examiners should, therefore, review the overall risk exposure to an organization. Specifically, examiners should be alert to situations in which the structure of a securitization obscures the concentration risk in individual ABS or in a portfolio of ABS. Examiners should also be mindful of structures that may effectively conceal low-quality assets or contingent liabilities from examination scrutiny and possible classification.
- Examiners should review a BO's insurance coverage to determine if it is sufficient to cover its fiduciary responsibilities under securitization arrangements. At least one rating agency requests that servicers carry errors and omissions insurance that will cover a minimum of 5 percent of the outstanding obligation.
- Private placements of ABS are not subject to the same legal-disclosure requirements as public placements. An organization involved in private placements of ABS should, therefore, exercise special caution with regard to disclosure of the risks and attributes of the securitized assets.

Banking Organizations Investing in ABS

ABS may appear similar to corporate notes; however, ABS possess many unique characteristics that affect their riskiness as investments. A BO should independently analyze all potential risk exposures before investing in ABS and should continue to monitor exposures throughout the life of the ABS. Analyses should focus

primarily on characteristics of ABS, such as credit risk, concentrations of exposures, interest-rate risk, liquidity risk, market risk, and prepayment risk. As an integral part of these analyses, a BO investing in ABS should evaluate the underlying assets, the participants in the securitization arrangement, and the structure of the securitization arrangement, although it should not be expected to analyze these factors in the same detail as BOs involved in the issuance of ABS.

Any purchase of ABS should be consistent with the overall objectives of the organization. The securities should constitute an integrated component of the investment or hedging plans of the organization and should not be purchased for speculative purposes. A banking organization should not rely on investment or trading strategies, which depend on the existence of liquid secondary ABS markets.

Policy and Portfolio Analysis

Credit risk. While ABS are often insulated, to some extent, from the credit risk of the underlying assets, credit risk is still affected by a number of factors, in addition to the performance of the underlying asset pool. These factors include the ability of the parties involved in the securitization arrangement to fulfill their obligations and the structure of the securitization itself.

In the event of default by obligors or other failure of the securitization structure, access to collateral may be difficult and recourse to the various providers of credit enhancement may be time-consuming and costly. Some forms of credit enhancement may be revocable. Banking organizations should not place undue reliance on collateral values and credit enhancement in evaluating ABS.

In many cases, ratings of the creditworthiness of ABS issues are available from external credit agencies. A banking organization may use credit ratings as a source of information, but should not depend solely on external agencies' evaluations of creditworthiness. Unrated ABS should be subject to particular scrutiny. Examiner procedures for reviewing credit risk are outlined below:

- Examiners should review a BO's policies and procedures to ensure that the organization follows prudent standards of credit assessment and has approval criteria for all ABS exposure. Procedures should include an initial thorough and independent credit assessment of ABS issues for which the organization has assumed any degree of credit risk, followed by periodic reviews to monitor performance of the ABS throughout the life of the exposure.
- Examiners should determine that a banking organization does not rely solely on conclusions of external rating services in evaluating ABS.
- Examiners should determine that a banking organization investing in ABS has independently made use of available documents in evaluating the credit risk of ABS. These documents include indentures, trustee reports, rating-agency bulletins, and prospectuses.
- Examiners should determine that a banking organization investing in privately placed ABS is aware of the differences in disclosure requirements between publicly placed and privately placed securities, and has taken extra steps to obtain and analyze information relevant to the evaluation of holdings of any privately placed ABS.
- Major policies and procedures, including internal credit-review and -approval procedures and in-house exposure limits, should be reviewed periodically and approved by the institution's board of directors.
- Failure, fraud, or mismanagement on the part of another party could result in loss to investors. A banking organization should have adequate procedures for assessing the financial strength and operational capacity of institutions involved in enhancing the credit quality of or managing an ABS issue.
- A banking organization should have procedures for evaluating the structural soundness of securitization arrangements for ABS in which it invests. The degree of investor control over transfer of servicing rights should be clearly delineated.
- Securitization arrangements may remove the ultimate investor from direct access to the collateral; the remedies available to an investor, in the event of default, should be clearly documented.

Concentration risk. Banking organizations may face concentrations of risk within the pool of assets, underlying an individual ABS issue, across different ABS issues, or through combinations of ABS and other credit exposures. Banking organizations that invest in ABS must

take special care to follow in-house diversification requirements for aggregate outstandings to a particular institution, industry, or geographic area. Examiner procedures for reviewing concentration risk are outlined below:

- When determining compliance with internal credit-exposure limits, securitization exposure should be aggregated with all loans, extensions of credit, debt and equity securities, legally binding financial guarantees and commitments, and any other investments involving the same obligor.
- Inherent in securitization is the risk that, if another party involved in the transaction becomes unable to perform, according to contract terms, the issue might default, even while the underlying credits are performing. Examiners should, therefore, ensure that, in addition to policies limiting direct credit exposure, an institution has developed exposure limits for particular credit enhancers, servicers, or trustees. Credit exposure to the other managing parties in a securitization should be included under a BO's general line to those institutions.
- Examiners should review the ABS portfolio for any industrial or geographic concentrations. Excessive exposures to a particular industry or region within the portfolio should be noted in the examiner's review.

Liquidity risk and market risk. Limited secondary markets may make ABS, especially unrated or innovative ABS, less liquid than many other debt instruments. Examiner procedures for reviewing liquidity and market risk are outlined below:

- If an investing bank is purchasing securitized assets for trading purposes, the examiner should ensure that the trading assets are carried at market value or at the lower of market or book value, and that market values are determined regularly. The risks involved are similar in character to the risks involved in trading other marketable securities. As with any trading activity, the BO must take proper steps to analyze market character and depth.
- A banking organization investing in ABS should not depend on secondary-market liquidity for the securities, especially in the case of ABS involving novel structures or innovative types of assets.
- Management information systems should provide management with timely and periodic information on the historical costs, market values, and unrealized gains and losses on ABS held in investment, trading, or resale portfolios.

Prepayment risk. The prepayment of assets underlying ABS may create prepayment risk for an investor in ABS. Prepayment risk may not be adequately reflected in agency ratings of ABS. Examiner procedures for reviewing prepayment risk are outlined below:

- Examiners should determine that a BO investing in ABS has analyzed the prepayment risk of ABS issues in its portfolio. Special care should be taken in the analysis of issues involving multiple tranches.
- Prepayment risk for ABS should be incorporated into an organization's net income-at-risk model, if such a model is used.

Legal Review

Examiners should review policies and procedures for compliance with applicable state lending limits and federal law, such as section 5136 of the Revised Codes. These requirements must be analyzed to determine whether a particular ABS issue is considered a single investment or a loan to each of the creditors underlying the pool. Collateralized mortgage obligations may be exempt from this limitation, if they are issued or guaranteed by an agency or instrumentality of the U.S. government.

Internal Audit and Management Information Systems

A BO's management of securitization risk depends on the providing of timely and accurate information about the organization's exposure to those responsible for monitoring risks. Examiners must be aware that a BO's involvement in asset securitization can be very extensive and place significant demands on systems without being readily evident, either as an on-balance-sheet exposure or a contingent liability. System overload or other technical default in the organization's systems could render the organization unable to provide proper monitoring or servicing. While the risk is not clearly associated with

the servicer (whose responsibility is long term and requires ongoing resource commitments), systems breakdowns may have risk implications for the credit enhancer and trustee. Examiners should ensure that internal auditors examine all facets of securitization regularly, as outlined below:

- Examiners should ensure that internal systems and controls adequately track the performance and condition of internal exposures and should monitor the organization's compliance with internal procedures and limits. In addition, adequate audit trails and internal-audit coverage should be provided.
- Cost-accounting systems should be adequate to permit a reliable determination of the profitability and volatility of asset-securitization activities.
- Management information systems and reporting procedures should be reviewed to determine that they—
  - — provide a listing of all securitizations for which the banking organization is either originator, servicer, credit enhancer, underwriter, trustee, or investor;
  - — provide concentration listings by industry and geographic area;
  - — generate information on total exposure to specific originators, servicers, credit enhancers, trustees, or underwriters;
  - — generate information on portfolio aging and performance relative to expectations; and
  - — provide periodic and timely information to senior management and directors on the organization's involvement in, and credit exposure arising from, securitization.

ADDITIONAL REFERENCES

The following is a list of accounting literature issued by FASB and the AICPA that relates to asset securitization or asset transfers.

FASB Statements

FASB Statement No. 5	Accounting for Contingencies
FASB Statement No. 6	Classification of Short-Term Obligations Expected to Be Refinanced
FASB Statement No. 48	Revenue Recognition When Right of Return Exists
FASB Statement No. 65	Accounting for Certain Mortgage Banking Enterprises, as amended
FASB Statement No. 66	Accounting for Sales of Real Estate
FASB Statement No. 77	Reporting by Transferors for Transfers of Receivables with Recourse
FASB Statement No. 91	Accounting for Nonrefundable Fees and Costs Associated with Originating or Acquiring Loans and Initial Direct Costs of Leases
FASB Statement No. 105	Disclosure of Information About Financial Instruments with Off-Balance-Sheet Risk and Financial Instruments with Concentrations of Credit Risk
FASB Statement No. 115	Accounting for Certain Investments in Debt and Equity Securities
FASB Statement No. 122	Accounting for Mortgage-Servicing Rights
FASB Statement No. 133	Accounting for Derivative Instruments and Hedging Activities
FASB Statement No. 134	Accounting for Mortgage-Backed Securities Retained After the Securitization of Mortgage Loans Held for Sale by a Mortgage Banking Enterprise
FASB Statement No. 137	Accounting for Derivative Instruments and Hedging Activities—Deferral of the Effective Date of FASB Statement No. 133 (an amendment of FASB Statement No. 133)
FASB Statement No. 138	Accounting for Certain Derivative Instruments and Hedging Activities (an amendment of FASB Statement No. 133)

FASB Statement No. 140 Accounting for Transfers and Servicing of Financial Assets and Extinguishments of Liabilities (a replacement of FASB Statement No. 125)
FASB Statement No. 149 Amendment of Statement 133 on Derivative Instruments and Hedging Activities
FASB Statement No. 150 Accounting for Certain Financial Instruments with Characteristics of Both Liabilities and Equity

FASB Interpretations

FIN 8 Classification of a Short-Term Obligation Repaid Prior to Being Replaced by a Long-Term Security
FIN 45 Guarantor's Accounting and Disclosure Requirements for Guarantees, Including Indirect Guarantees of Indebtedness of Others
FIN 46-R Consolidation of Variable Interest Entities

Technical Bulletins

TB 85-2 Accounting for Collateralized Mortgage Obligations
TB 87-3 Accounting for Mortgage Servicing Fees and Rights
TB 01-1 Effective Date for Certain Financial Institutions of Certain Provisions of Statement 140 Related to the Isolation of Transferred Financial Assets

EITF (Emerging Issues Task Force) Abstracts

84-15 Grantor Trusts Consolidation
84-21 Sale of a Loan with a Partial Participation Retained
84-30 Sales of Loans to Special-Purpose Entities
85-13 Sale of Mortgage-Service Rights on Mortgages Owned by Others
85-20 Recognition of Fees for Guaranteeing a Loan
85-26 Measurement of Servicing Fees Under FASB Statement No. 65 When a Loan Is Sold with Servicing Retained
85-28 Consolidation Issues Relating to Collateralized Mortgage Obligations
86-24 Third-Party Establishment of CMO
86-38 Implications of Mortgage Prepayments on Amortization of Servicing Rights
86-39 Gains from the Sale of Mortgage Loans with Servicing Rights Retained
87-25 Sales of Convertible, Adjustable-Rate Mortgages with Contingent Repayment Agreement
87-34 Sales of Mortgage-Servicing Rights with a Subservicing Agreement
88-11 Sale of Interest-Only or Principal-Only Cash Flows from Loans Receivable
88-17 Accounting for Fees and Costs Associated with Loan Syndications and Loan Participations
88-20 Difference Between Initial Investment and Principal Amount of Loans in a Purchased Credit-Card Portfolio
88-22 Securitization of Credit Card Portfolios
89-4 Collateralized Mortgage Obligation Residuals
89-5 Sale of Mortgage-Loan-Servicing Rights
89-18 Divestitures of Certain Investment Securities to an Unregulated Common Controlled Entity Under FIRREA
90-2 Exchange of Interest-Only or Principal-Only Securities for a Mortgage-Backed Security
90-18 Effect of a "Removal of Accounts" Provision on the Accounting for a Credit Card Securitization
93-18 Recognition for Impairment of an Investment in a Collateralized Mortgage Obligation Instrument or in a Mortgage-Backed Interest-Only Certificate

94-4 Classification of an Investment in a Mortgage-Backed Interest-Only Certificate as Held-to-Maturity
94-8 Accounting for Conversion of a Loan into a Debt Security in a Debt Restructuring
94-5 Determination of What Constitutes All Risks and Rewards and No Significant Unresolved Contingencies in a Sale of Mortgage-Loan-Servicing Rights
95-5 Determination of What Risks and Rewards, If Any, Can Be Retained and Whether Any Unresolved Contingencies May Exist in a Sale of Mortgage-Loan-Servicing Rights
D-39 Questions Related to the Implementation of FASB Statement No. 115
D-75 When to Recognize Gains and Losses on Assets Transferred to a Qualifying Special-Purpose Entity
D-94 Questions and Answers Related to the Implementation of FASB Statement No. 140
D-99 Questions and Answers Related to Servicing Activities in a Qualifying Special-Purpose Entity Under FASB Statement No. 140

AICPA Statements of Position

90-3 Definition of the Term "Substantially the Same" for Holders of Debt Instruments, as Used in Certain Audit Guides and a Statement of Position
94-6 Disclosure of Certain Significant Risks and Uncertainties

1. To determine if the bank is in compliance with laws, regulations, and policy statements.
2. To determine if the bank has originated, serviced, credit-enhanced, served as a trustee for, or invested in securitized assets.
3. To determine that securitization activities are integrated into the overall strategic objectives of the organization.
4. To determine that management has an appropriate level of experience in securitization activities.
5. To ensure that the bank does not hold any asset-backed securities that are inappropriate, for example, interest-only strips (IOs) and principal-only strips (POs), given the size of the bank and the sophistication of its operations.
6. To ensure that all asset-backed securities owned, any assets sold with recourse, retained interests, and variable interest entities (VIEs) (for example, asset-backed commercial paper (ABCP) programs that are defined as VIEs under GAAP) are properly accounted for on the bank's books and are correctly reported on the bank's regulatory reports.
7. To determine that sources of credit risk are understood, properly analyzed, and managed, without excessive reliance on credit ratings by outside agencies.
8. To determine that credit, operational, and other risks are recognized and addressed through appropriate policies, procedures, management reports, and other controls.
9. To determine if officers are operating in conformance with established bank policies and procedures.
10. To determine whether liquidity and market risks are recognized and whether the organization is excessively dependent on securitization as a substitute for day-to-day core funding or as a source of income.
11. To determine that steps have been taken to minimize the potential for conflicts of interest arising from the institution's securitization activities.
12. To determine that possible sources of structural failure in securitization transactions are recognized and that the organization has adopted measures to minimize the impact of these failures if they occur.
13. To determine that the organization is aware of the legal risks and uncertainty of various aspects of securitization.
14. To determine that concentrations of exposure in the underlying asset pools, asset-backed securities portfolio, or structural elements of securitization transactions are avoided.
15. To determine that all sources of risk are evaluated at the inception of each securitization activity and are monitored on an ongoing basis.
16. To determine whether the institution's retained interests from asset securitization are properly documented, valued, and accounted for.
17. To verify that the amount of retained interests not supported by adequate documentation has been charged off and that the assets involved in those retained interests are not used for risk-based calculation purposes.
18. To ascertain the existence of sound risk modeling, management information systems (MIS), and disclosure practices for asset securitization.
19. To obtain assurances that the board of directors and management oversee sound policies and internal controls concerning the recording of asset-securitization transactions and any valuation of retained interests derived therefrom.
20. To determine that capital is commensurate with, and that there are accurate determinations of, the risk weights for the risk exposures arising from recourse obligations, direct-credit substitutes, asset- and mortgage-backed securities, ABCP programs and ABCP liquidity facilities, and other asset-securitization transactions.
21. To determine whether there is an independent audit function that is capable of evaluating asset-securitization activities and any associated retained interests.
22. To initiate corrective action if policies, practices, procedures, or internal controls are deficient or when violations of law, regulations, or policy statements are disclosed.

1. a. Request a schedule of all asset-backed securities owned by the bank. Reconcile the balance of these assets to the subsidiary ledgers of the balance sheet, and review credit ratings assigned to these securities by independent rating agencies. Determine that the accounting methods and procedures used for these assets, at inception and throughout the carrying life, are appropriate.
   b. Request and review information on the types and amount of assets that have been securitized by the bank. In addition, request information concerning potential contractual or contingent liability arising from any guarantees, underwriting, and servicing of the securitized assets.
2. Review the parent company's policies and procedures to ensure that its banking and nonbanking subsidiaries follow prudent standards of credit assessment and approval for all securitization exposure. Procedures should include a thorough and independent credit assessment of each loan or pool for which it has assumed credit risk, followed by periodic credit reviews to monitor performance throughout the life of the exposure. If a banking organization (BO) invests in asset-backed securities (ABS), determine whether it relies soley on conclusions of external rating services when evaluating the securities.
3. Determine that rigorous credit standards are applied regardless of the role the organization plays in the securitization process, for example, servicer, credit enhancer, or investor.
4. Determine that major policies and procedures, including internal credit-review and credit-approval procedures and "in-house" exposure limits, are reviewed periodically and approved by the bank's board of directors.
5. Determine whether adequate procedures for evaluating the organization's internal control procedures and the financial strength of the other institutions involved in the securitization process are in place.
6. Obtain the documentation outlining the remedies available to provide credit enhancement in the event of a default. Both originators and purchasers of securitized assets should have prospectuses on the issue. Obtaining a copy of the prospectus can be an invaluable source of information. Prospectuses generally contain information on credit enhancement, default provisions, subordination agreements, etc. In addition to the prospectus, obtain the documentation confirming the purchase or sale of a security.
7. Ensure that, regardless of the role an institution plays in securitization, the documentation for an asset-backed security clearly specifies the limitations of the institution's legal responsibility to assume losses.
8. Determine the existence of independent risk-management processes and management information systems (MIS). Determine whether these processes and systems are being used to monitor securitization-pool performance on an aggregate and individual transaction level.
9. Verify whether the BO, acting as originator, packager, or underwriter, has written policies addressing the repurchase of assets and other measures to reimburse investors in the event that a defaulted package results in losses exceeding any contractual credit enhancement. The repurchase of defaulted assets or pools in contradiction of or outside the terms of the underlying agreement in effect sets a standard by which a banking organization could potentially be found legally liable for all "sold" assets. Review and report any situations in which the organization has repurchased or otherwise reimbursed investors for poor-quality assets.
10. Classify adverse credit risk associated with the securitization of assets when analyzing the adequacy of an organization's capital or reserve levels. Evaluate credit risk of ABS, and classify any adverse credit risk. List classified assets. Evaluate the impact of the classification on capital adequacy and the overall soundness of the institution.
11. Aggregate securitization exposures with all loans, extensions of credit, debt and equity securities, legally binding financial guarantees and commitments, and any other investments involving the same obligor when

determining compliance with internal credit-exposure limits.

12. Review the bank's valuation assumptions and modeling methodology used for ABS to determine if they are conservative and appropriate and are being used to establish, evaluate, and adjust the carrying value of retained interests on a regular and timely basis.
13. Determine if audit or internal-review staffs periodically review data integrity, model algorithms, key underlying assumptions, and the appropriateness of the valuation and modeling process for the securitized assets that the institution retains.
14. Review the risk-based capital calculations, and determine if they include recognition and the correct reporting of any recourse obligations, direct-credit substitutes, residual interests, asset- and mortgage-backed securities, asset-backed commercial paper (ABCP) programs, liquidity facilities, and other transactions involving such securitization activities.
15. Determine if the bank consolidates, in accordance with GAAP (FASB's Statement of Financial Accounting Standards No. 167, "Amendments to FASB Interpretation No. 146(R)(FAS 167)" the assets of any ABCP program or other such program that it sponsors.
    a. Determine if the bank's ABCP program met the definition of a sponsored ABCP program under the risk-based capital guidelines.
    b. Ascertain whether the liquidity facilities the bank extends to the ABCP program satisfy the risk-based capital definition and requirements, including the appropriate asset-quality test, of an eligible ABCP program liquidity facility. (See 12 CFR 208, appendix A, III.B.3.a.iv.)
    c. Determine whether the bank applied the correct credit-conversion factor to eligible ABCP liquidity facilities when it determined the amount of risk-weighted assets for its risk-based capital ratios. (See 12 CFR 208, appendix A, section III.D.)
    d. Determine if all ineligible ABCP liquidity facilities were treated as either direct-credit substitutes or as recourse obligations, as required by the risk-based capital guidelines.
    e. If the bank had multiple positions with overlapping exposures, determine if the bank applied the risk-based capital treatment that resulted in the highest capital charge. (See 12 CFR, appendix A, section III.B.6.c.)
16. Ascertain that internal limits govern the amount of retained interests held as a percentage of total equity capital.
17. Establish that an adequate liquidity contingency plan is in place and will be used in the event of market disruptions. Determine whether liquidity problems may arise as the result of an overdependence on asset-securitization activities for day-to-day core funding.
18. Determine whether consistent, conservative accounting practices are in place that satisfy the reporting requirements of regulatory supervisors, GAAP reporting requirements, and valuation assumptions and methods. Ascertain that adequate disclosures of asset-securitization activities are made commensurate with the volume of securitizations and the complexities of the institution.
19. Establish that risk-exposure limits and requirements exist and are adhered to on an aggregate and individual transaction basis.
20. Review securitized assets for industrial or geographic concentrations. Excessive exposures to an industry or region among the underlying assets should be noted in the review of the loan portfolio.
21. Ensure that, in addition to policies limiting direct credit exposure, an institution has developed exposure limits for particular originators, credit enhancers, trustees, and servicers.
22. Review the policies of the banking organization engaged in underwriting, watching for situations in which it cannot sell underwritten asset-backed securities. Credit review, funding capabilities, and approval limits should allow the institution to purchase and hold unsold securities. All potential credit exposure should be within legal lending limits.
23. Ensure that internal systems and controls adequately track the performance and condition of internal exposures and monitor the organization's compliance with internal procedures and limits. In addition, adequate audit trails and internal audit coverage should be provided. Ensure that the reports have adequate scope and frequency of detail.

24. Determine that management information systems provide—
    a. a listing of each securitization transaction in which the organization is involved;
    b. a listing of industry and geographic concentrations;
    c. information on total exposure to specific originators, servicers, credit enhancers, trustees, or underwriters;
    d. information regarding portfolio monthly vintage or aging and information on a portfolio's performance by specific product type relative to expectations;
    e. periodic and timely information to senior management and directors on the organization's involvement in, and credit exposure arising from, securitization;
    f. static-pool cash-collection analysis;
    g. sensitivity analysis; and
    h. a statement of covenant compliance.
25. Ensure that internal auditors examine all facets of securitization regularly.
26. Review policies and procedures for compliance with applicable state lending limits and federal law, such as section 5136 of the Revised Codes. These requirements must be analyzed to determine whether a particular asset-backed-security issue is considered a single investment or a loan to each of the creditors underlying the pool. Collateralized mortgage obligations may be exempt from this limitation, if they are issued or guaranteed by an agency or instrumentality of the U.S. government.
27. Determine whether the underwriting of ABS of affiliates is—
    a. rated by an unaffiliated, nationally recognized statistical rating organization; or
    b. issued or guaranteed by Fannie Mae, FHLMC, or GNMA, or represents interests in such obligations.
28. Determine if purchases of high-risk mortgage-backed securities were made to reduce the overall interest-rate risk of the bank. Determine if the bank evaluates and documents at least quarterly whether these securities have reduced the interest-rate risk.
29. Review and discuss any documentation exceptions, violations, internal control exceptions, and classifications with management, and obtain management's response.
30. Review the bank's liquidity agreements with any asset-backed commercial paper programs and determine whether the agreements have any credit-related components. Is the bank required to purchase the assets? Are these assets repurchased from the bank? If the facility is determined to be a commitment, determine whether its maturity is short term or long term. Do any of the liquidity agreements contain a material adverse clause or any other credit-contingency provision?

Review the bank's internal controls, policies, practices, and procedures for all aspects of asset securitization. The bank's system should be documented completely and concisely and should include, where appropriate, narrative descriptions, flow charts, copies of forms used, and other pertinent information.

POLICIES

1. Does the bank employ the services of a securities dealer? If so, does the bank rely solely on the advice of such dealer when purchasing asset-backed securities for the bank's investment portfolio? Does the bank have persons who are responsible for reviewing or approving the investment manager's acquisitions? Are minimum criteria established for selecting a securities dealer?
2. Has the board of directors, consistent with its duties and responsibilities, reviewed and ratified asset-securitization policies, practices, and procedures? Do these policies, practices, and procedures—
   a. require an initial thorough and independent credit assessment of each pool for which the bank has assumed credit risk, as either a participant in the securitization process or as an investor?
   b. address the bank's repurchase of assets and other forms of reimbursement to investors, when the bank is acting as the originator, packager, or underwriter, in the event that a default results in losses exceeding any contractual credit enhancement?
   c. ensure that the credit, pricing, and servicing standards for securitized assets are equivalent to standards for assets that remain on the bank's books?
   d. ensure that the credit, pricing, and servicing standards and that compliance with any provisions relating to government guarantees are reviewed periodically by the board of directors?
   e. establish in-house diversification requirements for aggregate outstanding exposures to a particular institution, industry, or geographic area?
   f. hedge the bank's exposure to adverse price movements when it is engaged in underwriting or market-making activities?
3. Are the bank's securitization policies reviewed and reaffirmed at least annually to determine if they are compatible with changing market conditions?

INTERNAL CONTROL AND MANAGEMENT INFORMATION SYSTEMS

1. Do the internal systems and controls adequately track the performance and condition of internal exposures, and do the systems monitor the bank's compliance with internal procedures and limits? Are adequate audit trails and internal audit coverage provided?
2. Do the cost accounting systems provide a reliable determination of the profitability and volatility of asset-securitization activities?
3. Are management information systems and reporting procedures adequate in that they provide—
   a. a listing of all securitizations for which the bank is either originator, servicer, credit enhancer, underwriter, or trustee?
   b. a listing of industry and geographic concentrations?
   c. information on total exposure to specific originators, servicers, credit enhancers, trustees, or underwriters?
   d. information regarding portfolio aging and performance relative to expectations?
   e. periodic and timely information to senior management and directors on the organization's involvement in, and credit exposure arising from, securitization?
   f. credit ratings assigned by independent rating agencies to all asset-backed securities held by the bank?
4. Do management information systems and reporting procedures adequately document the bank's calculation and determination of risk-based capital ratios (including the assignment of the appropriate risk-based capital charges (risk weights and credit-conversion factors)) against the exposures arising from asset-backed and mortgage-backed securitization transactions or activities, including asset-backed commercial paper programs

(including exposures arising from direct-credit substitutes, recourse obligations, residual interests, liquidity facilities, and mortgage-backed and other types of asset-backed loans)?

This section sets forth the Interagency Statement on Sound Practices Concerning Elevated-Risk Complex Structured Finance Activities, issued January 11, 2007.[1] The supervisory guidance addresses risk-management principles that should assist institutions to identify, evaluate, and manage the heightened legal and reputational risks that may arise from their involvement in complex structured finance transactions (CSFTs). The guidance is focused on sound practices related to CSFTs that may create heightened legal or reputational risks to the institution and are defined as "elevated-risk CSFTs." Such transactions are typically conducted by a limited number of large financial institutions.[2] (See SR-07-05.)

INTERAGENCY STATEMENT ON SOUND PRACTICES CONCERNING ELEVATED-RISK COMPLEX STRUCTURED FINANCE ACTIVITIES

Financial markets have grown rapidly over the past decade, and innovations in financial instruments have facilitated the structuring of cash flows and allocation of risk among creditors, borrowers, and investors in more efficient ways. Financial derivatives for market and credit risk, asset-backed securities with customized cash-flow features, specialized financial conduits that manage pools of assets, and other types of structured finance transactions serve important business purposes, such as diversifying risks, allocating cash flows, and reducing cost of capital. As a result, structured finance transactions have become an essential part of U.S. and international capital markets. Financial institutions have played and continue to play an active and important role in the development of structured finance products and markets, including the market for the more complex variations of structured finance products.

When a financial institution[3] participates in a CSFT, it bears the usual market, credit, and operational risks associated with the transaction. In some circumstances, a financial institution also may face heightened legal or reputational risks due to its involvement in a CSFT. For example, in some circumstances, a financial institution may face heightened legal or reputational risk if a customer's regulatory, tax, or accounting treatment for a CSFT, or disclosures to investors concerning the CSFT in the customer's public filings or financial statements, do not comply with applicable laws, regulations, or accounting principles. Indeed, in some instances, CSFTs have been used to misrepresent a customer's financial condition to investors, regulatory authorities, and others. In these situations, investors have been harmed and financial institutions have incurred significant legal and reputational exposure. In addition to legal risk, reputational risk poses a significant threat to financial institutions because the nature of their business requires them to maintain the confidence of customers, creditors, and the general marketplace.

The agencies[4] have long expected financial institutions to develop and maintain robust control infrastructures that enable them to identify, evaluate, and address the risks associated with their business activities. Financial institutions also must conduct their activities in accordance with applicable statutes and regulations.

Scope and Purpose of Statement

The agencies issued this statement to describe the types of risk-management principles they believe may help a financial institution to identify CSFTs that may pose heightened legal or reputational risks to the institution and to evalu-

1. See 72 *Fed. Reg.* 1372, January 11, 2007.

2. The statement will not affect or apply to the vast majority of financial institutions, including most small institutions.

3. As used in this statement, the term *financial institution* or *institution* refers to state member banks and bank holding companies (other than foreign banking organizations) in the case of the Board of Governors of the Federal Reserve System (FRB); to national banks in the case of the Office of the Comptroller of the Currency (OCC); to federal and state savings associations and savings and loan holding companies in the case of the Office of Thrift Supervision (OTS); to state nonmember banks in the case of the Federal Deposit Insurance Corporation (FDIC); and to registered broker-dealers and investment advisers in the case of the Securities and Exchange Commission (SEC). The U.S. branches and agencies of foreign banks supervised by the FRB, the OCC, and the FDIC also are considered to be financial institutions for purposes of this statement.

4. The federal banking agencies (the FRB, the OCC, the FDIC, and the OTS) and the SEC.

ate, manage, and address these risks within the institution's internal control framework.

Structured finance transactions encompass a broad array of products with varying levels of complexity. Most structured finance transactions, such as standard public mortgage-backed securities transactions, public securitizations of retail credit cards, asset-backed commercial paper conduit transactions, and hedging-type transactions involving "plain vanilla" derivatives and collateralized loan obligations, are familiar to participants in the financial markets, and these vehicles have a well-established track record. These transactions typically would not be considered CSFTs for the purpose of this statement.

Because this statement focuses on sound practices related to CSFTs that may create heightened legal or reputational risks—transactions that typically are conducted by a limited number of large financial institutions—it will not affect or apply to the vast majority of financial institutions, including most small institutions. As in all cases, a financial institution should tailor its internal controls so that they are appropriate in light of the nature, scope, complexity, and risks of its activities. Thus, for example, an institution that is actively involved in structuring and offering CSFTs that may create heightened legal or reputational risk for the institution should have a more formalized and detailed control framework than an institution that participates in these types of transactions less frequently. The internal controls and procedures discussed in this statement are not all-inclusive, and, in appropriate circumstances, an institution may find that other controls, policies, or procedures are appropriate in light of its particular CSFT activities.

Because many of the core elements of an effective control infrastructure are the same regardless of the business line involved, this statement draws heavily on controls and procedures that the agencies previously have found to be effective in assisting a financial institution to manage and control risks and identifies ways in which these controls and procedures can be effectively applied to elevated-risk CSFTs. Although this statement highlights some of the most significant risks associated with elevated-risk CSFTs, it is not intended to present a full exposition of all risks associated with these transactions. Financial institutions are encouraged to refer to other supervisory guidance prepared by the agencies for further information concerning market, credit, operational, legal, and reputational risks as well as internal audit and other appropriate internal controls.

This statement does not create any private rights of action and does not alter or expand the legal duties and obligations that a financial institution may have to a customer, its shareholders, or other third parties under applicable law. At the same time, adherence to the principles discussed in this statement would not necessarily insulate a financial institution from regulatory action or any liability the institution may have to third parties under applicable law.

Identification and Review of Elevated-Risk CSFTs

A financial institution that engages in CSFTs should maintain a set of formal, written, firm-wide policies and procedures that are designed to allow the institution to identify, evaluate, assess, document, and control the full range of credit, market, operational, legal, and reputational risks associated with these transactions. These policies may be developed specifically for CSFTs, or included in the set of broader policies governing the institution generally. A financial institution operating in foreign jurisdictions may tailor its policies and procedures as appropriate to account for, and comply with, the applicable laws, regulations, and standards of those jurisdictions.[5]

A financial institution's policies and procedures should establish a clear framework for the review and approval of individual CSFTs. These policies and procedures should set forth the responsibilities of the personnel involved in the origination, structuring, trading, review, approval, documentation, verification, and execution of CSFTs. Financial institutions may find it helpful to incorporate the review of new CSFTs into their existing new-product policies. In this regard, a financial institution should define what constitutes a "new" complex structured finance product and establish a control process for the approval of such new products. In determining

5. In the case of U.S. branches and agencies of foreign banks, these policies, including management, review, and approval requirements, should be coordinated with the foreign bank's group-wide policies developed in accordance with the rules of the foreign bank's home-country supervisor and should be consistent with the foreign bank's overall corporate and management structure as well as its framework for risk management and internal controls.

whether a CSFT is new, a financial institution may consider a variety of factors, including whether it contains structural or pricing variations from existing products; whether the product is targeted at a new class of customers; whether it is designed to address a new need of customers; whether it raises significant new legal, compliance, or regulatory issues; and whether it or the manner in which it would be offered would materially deviate from standard market practices. An institution's policies should require new complex structured finance products to receive the approval of all relevant control areas that are independent of the profit center before the product is offered to customers.

Identifying Elevated-Risk CSFTs

As part of its transaction and new-product approval controls, a financial institution should establish and maintain policies, procedures, and systems to identify elevated-risk CSFTs. Because of the potential risks they present to the institution, transactions or new products identified as elevated-risk CSFTs should be subject to heightened reviews during the institution's transaction or new-product approval processes. Examples of transactions that an institution may determine warrant this additional scrutiny are those that (either individually or collectively) appear to the institution during the ordinary course of its transaction approval or new-product approval process to—

- lack economic substance or business purpose;
- be designed or used primarily for questionable accounting, regulatory, or tax objectives, particularly when the transactions are executed at year-end or at the end of a reporting period for the customer;
- raise concerns that the client will report or disclose the transaction in its public filings or financial statements in a manner that is materially misleading or inconsistent with the substance of the transaction or applicable regulatory or accounting requirements;
- involve circular transfers of risk (either between the financial institution and the customer or between the customer and other related parties) that lack economic substance or business purpose;
- involve oral or undocumented agreements that, when taken into account, would have a material impact on the regulatory, tax, or accounting treatment of the related transaction, or the client's disclosure obligations;[6]
- have material economic terms that are inconsistent with market norms (for example, deep "in the money" options or historic rate rollovers); or
- provide the financial institution with compensation that appears substantially disproportionate to the services provided or investment made by the financial institution or to the credit, market, or operational risk assumed by the institution.

The examples listed previously are provided for illustrative purposes only, and the policies and procedures established by financial institutions may differ in how they seek to identify elevated-risk CSFTs. The goal of each institution's policies and procedures, however, should remain the same: to identify those CSFTs that warrant additional scrutiny in the transaction or new-product approval process due to concerns regarding legal or reputational risks.

Financial institutions that structure or market, act as an advisor to a customer regarding, or otherwise play a substantial role in a transaction may have more information concerning the customer's business purpose for the transaction and any special accounting, tax, or financial disclosure issues raised by the transaction than institutions that play a more limited role. Thus, the ability of a financial institution to identify the risks associated with an elevated-risk CSFT may differ depending on its role.

Due Diligence, Approval, and Documentation Process for Elevated-Risk CSFTs

Having developed a process to identify elevated-risk CSFTs, a financial institution should implement policies and procedures to conduct a heightened level of due diligence for these transactions. The financial institution should design these policies and procedures to allow personnel at an appropriate level to understand and evaluate the potential legal or reputational risks presented by

6. This item is not intended to include traditional, nonbinding "comfort" letters or assurances provided to financial institutions in the loan process where, for example, the parent of a loan customer states that the customer (i.e., the parent's subsidiary) is an integral and important part of the parent's operations.

the transaction to the institution and to manage and address any heightened legal or reputational risks ultimately found to exist with the transaction.

Due diligence. If a CSFT is identified as an elevated-risk CSFT, the institution should carefully evaluate and take appropriate steps to address the risks presented by the transaction, with a particular focus on those issues identified as potentially creating heightened levels of legal or reputational risk for the institution. In general, a financial institution should conduct the level and amount of due diligence for an elevated-risk CSFT that is commensurate with the level of risks identified. A financial institution that structures or markets an elevated-risk CSFT to a customer, or that acts as an advisor to a customer or investors concerning an elevated-risk CSFT, may have additional responsibilities under the federal securities laws, the Internal Revenue Code, state fiduciary laws, or other laws or regulations and, thus, may have greater legal- and reputational-risk exposure with respect to an elevated-risk CSFT than a financial institution that acts only as a counterparty for the transaction. Accordingly, a financial institution may need to exercise a higher degree of care in conducting its due diligence when the institution structures or markets an elevated-risk CSFT or acts as an advisor concerning such a transaction than when the institution plays a more limited role in the transaction.

To appropriately understand and evaluate the potential legal and reputational risks associated with an elevated-risk CSFT that a financial institution has identified, the institution may find it useful or necessary to obtain additional information from the customer or to obtain specialized advice from qualified in-house or outside accounting, tax, legal, or other professionals. As with any transaction, an institution should obtain satisfactory responses to its material questions and concerns prior to consummation of a transaction.[7]

In conducting its due diligence for an elevated-risk CSFT, a financial institution should independently analyze the potential risks to the institution from both the transaction and the institution's overall relationship with the customer. Institutions should not conclude that a transaction identified as being an elevated-risk CSFT involves minimal or manageable risks solely because another financial institution will participate in the transaction or because of the size or sophistication of the customer or counterparty. Moreover, a financial institution should carefully consider whether it would be appropriate to rely on opinions or analyses prepared by or for the customer concerning any significant accounting, tax, or legal issues associated with an elevated-risk CSFT.

Approval process. A financial institution's policies and procedures should provide that CSFTs identified as having elevated legal or reputational risk are reviewed and approved by appropriate levels of control and management personnel. The designated approval process for such CSFTs should include representatives from the relevant business line(s) and/or client management, as well as from appropriate control areas that are independent of the business line(s) involved in the transaction. The personnel responsible for approving an elevated-risk CSFT on behalf of a financial institution should have sufficient experience, training, and stature within the organization to evaluate the legal and reputational risks, as well as the credit, market, and operational risks to the institution.

The institution's control framework should have procedures to deliver the necessary or appropriate information to the personnel responsible for reviewing or approving an elevated-risk CSFT to allow them to properly perform their duties. Such information may include, for example, the material terms of the transaction, a summary of the institution's relationship with the customer, and a discussion of the significant legal, reputational, credit, market, and operational risks presented by the transaction.

Some institutions have established a senior management committee that is designed to involve experienced business executives and senior representatives from all of the relevant control functions within the financial institution (including such groups as independent risk management, tax, accounting, policy, legal, compliance, and financial control) in the oversight and approval of those elevated-risk CSFTs that are identified by the institution's personnel as requiring senior management review and approval due to the potential risks associated with the transactions. While this type of management committee may not be appropriate for all financial institutions, a financial institution should establish processes that assist the institution in con-

7. Of course, financial institutions also should ensure that their own accounting for transactions complies with applicable accounting standards, consistently applied.

sistently managing the review and approval of elevated-risk CSFTs on a firm-wide basis.[8]

If, after evaluating an elevated-risk CSFT, the financial institution determines that its participation in the CSFT would create significant legal or reputational risks for the institution, the institution should take appropriate steps to address those risks. Such actions may include declining to participate in the transaction, or conditioning its participation upon the receipt of representations or assurances from the customer that reasonably address the heightened legal or reputational risks presented by the transaction. Any representations or assurances provided by a customer should be obtained before a transaction is executed and be received from, or approved by, an appropriate level of the customer's management. A financial institution should decline to participate in an elevated-risk CSFT if, after conducting appropriate due diligence and taking appropriate steps to address the risks from the transaction, the institution determines that the transaction presents unacceptable risk to the institution or would result in a violation of applicable laws, regulations, or accounting principles.

Documentation. The documentation that financial institutions use to support CSFTs is often highly customized for individual transactions and negotiated with the customer. Careful generation, collection, and retention of documents associated with elevated-risk CSFTs are important control mechanisms that may help an institution monitor and manage the legal, reputational, operational, market, and credit risks associated with the transactions. In addition, sound documentation practices may help reduce unwarranted exposure to the financial institution's reputation.

A financial institution should create and collect sufficient documentation to allow the institution to—

- document the material terms of the transaction;
- enforce the material obligations of the counterparties;
- confirm that the institution has provided the customer any disclosures concerning the transaction that the institution is otherwise required to provide; and
- verify that the institution's policies and procedures are being followed and allow the internal audit function to monitor compliance with those policies and procedures.

When an institution's policies and procedures require an elevated-risk CSFT to be submitted for approval to senior management, the institution should maintain the transaction-related documentation provided to senior management as well as other documentation, such as minutes of the relevant senior management committee, that reflect senior management's approval (or disapproval) of the transaction, any conditions imposed by senior management, and the factors considered in taking such action. The institution should retain documents created for elevated-risk CSFTs in accordance with its record retention policies and procedures as well as applicable statutes and regulations.

Other Risk-Management Principles for Elevated-Risk CSFTs

General business ethics. The board and senior management of a financial institution also should establish a "tone at the top" through both actions and formalized policies that sends a strong message throughout the financial institution about the importance of compliance with the law and overall good business ethics. The board and senior management should strive to create a firm-wide corporate culture that is sensitive to ethical or legal issues as well as the potential risks to the financial institution that may arise from unethical or illegal behavior. This kind of culture coupled with appropriate procedures should reinforce business-line ownership of risk identification and encourage personnel to move ethical or legal concerns regarding elevated-risk CSFTs to appropriate levels of management. In appropriate circumstances, financial institutions may also need to consider implementing mechanisms to protect personnel by permitting the confidential disclosure of concerns.[9] As in other areas of financial institution

8. The control processes that a financial institution establishes for CSFTs should take account of, and be consistent with, any informational barriers established by the institution to manage potential conflicts of interest, insider trading, or other concerns.

9. The agencies note that the Sarbanes-Oxley Act of 2002 requires companies listed on a national securities exchange or inter-dealer quotation system of a national securities association to establish procedures that enable employees to submit

management, compensation and incentive plans should be structured, in the context of elevated-risk CSFTs, so that they provide personnel with appropriate incentives to have due regard for the legal-, ethical-, and reputational-risk interests of the institution.

Reporting. A financial institution's policies and procedures should provide for the appropriate levels of management and the board of directors to receive sufficient information and reports concerning the institution's elevated-risk CSFTs to perform their oversight functions.

Monitoring compliance with internal policies and procedures. The events of recent years evidence the need for an effective oversight and review program for elevated-risk CSFTs. A financial institution's program should provide for periodic independent reviews of its CSFT activities to verify and monitor that its policies and controls relating to elevated-risk CSFTs are being implemented effectively and that elevated-risk CSFTs are accurately identified and have received proper approvals. These independent reviews should be performed by appropriately qualified audit, compliance, or other personnel in a manner consistent with the institution's overall framework for compliance monitoring, which should include consideration of issues such as the independence of reviewing personnel from the business line. Such monitoring may include more-frequent assessments of the risk arising from elevated-risk CSFTs, both individually and within the context of the overall customer relationship, and the results of this monitoring should be provided to an appropriate level of management in the financial institution.

Audit. The internal audit department of any financial institution is integral to its defense against fraud, unauthorized risk taking, and damage to the financial institution's reputation. The internal audit department of a financial institution should regularly audit the financial institution's adherence to its own control procedures relating to elevated-risk CSFTs, and further assess the adequacy of its policies and procedures related to elevated-risk CSFTs. Internal audit should periodically validate that business lines and individual employees are complying with the financial institution's standards for elevated-risk CSFTs and appropriately identifying any exceptions. This validation should include transaction testing for elevated-risk CSFTs.

Training. An institution should identify relevant personnel who may need specialized training regarding CSFTs to be able to effectively perform their oversight and review responsibilities. Appropriate training on the financial institution's policies and procedures for handling elevated-risk CSFTs is critical. Financial institution personnel involved in CSFTs should be familiar with the institution's policies and procedures concerning elevated-risk CSFTs, including the processes established by the institution for identification and approval of elevated-risk CSFTs and new complex structured finance products and for the elevation of concerns regarding transactions or products to appropriate levels of management. Financial institution personnel involved in CSFTs should be trained to identify and properly handle elevated-risk CSFTs that may result in a violation of law.

CONCLUSION

Structured finance products have become an essential and important part of the U.S. and international capital markets, and financial institutions have played an important role in the development of structured finance markets. In some instances, however, CSFTs have been used to misrepresent a customer's financial condition to investors and others, and financial institutions involved in these transactions have sustained significant legal and reputational harm. In light of the potential legal and reputational risks associated with CSFTs, a financial institution should have effective risk-management and internal control systems that are designed to allow the institution to identify elevated-risk CSFTs; to evaluate, manage, and address the risks arising from such transactions; and to conduct those activities in compliance with applicable law.

concerns regarding questionable accounting or auditing matters on a confidential, anonymous basis. (See 15 USC 78j-1(m).)

Bank management is responsible for controlling risk at a level deemed acceptable for the organization. An effective risk-management program begins with the identification of exposures that could disrupt the timely and accurate delivery of business services or result in unexpected financial claims on bank resources. Risk management also involves the implementation of cost-effective controls and the shifting, transfer, or assignment of risk to third parties through insurance coverage or other risk-transfer techniques. Although the design and sophistication of risk-management procedures varies from bank to bank, each institution's decision-making process should effectively identify; control; and, when or where appropriate, result in some transfer of risk. The risk-assessment program should be conducted annually to establish whether potential service disruptions and estimated risk-related financial costs and losses can be contained at levels deemed acceptable to bank management and the board of directors. Note that insurance can provide a bank with the resources to restore business operations and financial stability only *after* an unanticipated event has occurred, but a bank's own risk-management controls can prevent and minimize losses before they occur.

RISK-MANAGEMENT PROGRAM

A sound operational risk-management program requires the annual review of all existing business operations and a risk assessment of all proposed services. Identified risks should be analyzed to estimate their potential and probable levels of loss exposure. While the historical loss experience of the bank and other service providers may be helpful in quantifying loss exposure, technological and societal changes may result in exposure levels that differ from historical experience. Nevertheless, current exposure estimates should be derived from the bank's historical loss experience and augmented with industry experience. In addition, the bank's insurance broker or agent should be a source of advice.

Management must decide the most appropriate method for addressing a particular risk. Although many factors influence this decision, the purpose of risk management is to minimize the probability of losses and the net costs associated with them. In that context, cost is broadly defined to include—

- the direct and consequential cost of loss-prevention measures (controls), plus
- insurance premiums, plus
- losses sustained, including the consequential effects and expenses to reduce such losses, minus
- recoveries from third parties and indemnities from insurers on account of such losses, plus
- pertinent administrative costs.

Bank risks with potentially high or even catastrophic financial consequences should be eliminated or substantially mitigated whenever possible, even when the risk's frequency of occurrence is low. These risks can be eliminated by discontinuing operations where appropriate or by assigning the risk exposure to other parties using third-party service providers. When the exposure cannot be shifted to other parties or otherwise mitigated, the bank must protect itself with appropriate levels of insurance. Certain loss exposures may be deemed reasonable because their probability of frequency and severity of loss are low, the level of expected financial loss or service disruption is minimal, or the costs associated with the recovery of assets and restoration of services are low.

Bank management may decide to reduce insurance premiums and claims-processing costs by self-insuring for various types of losses, setting higher deductible levels, lowering the coverage limits for insurance purchased, and narrowing coverage terms and conditions. A financial organization's primary defenses against loss are adequate internal controls and procedures, which insurance is intended to complement, not replace. Thus, an overall appraisal of the organization's control environment is a significant consideration in determining the adequacy of the insurance program. To the extent that controls are lacking, the need for additional insurance coverage increases. These determinations should be based on the results of the risk assessment and be consistent with the limits established by the board of directors. Insurance decisions may also be influenced by the insurance broker's advice regarding current insurance market and premium trends.

Following September 2001, insurance companies reevaluated their position on providing coverage for acts of terrorism. As a result, terrorism coverage has become expensive or unavailable. The bank's "schedule of insurance" should note which policies contain exclusions, sublimits, or large deductibles for losses incurred as a result of terrorism.

When selecting insurance carriers, banks should consider the financial strength and claims-paying capacity of the insurance underwriter, as well as the robustness or strength of the supervisory regime to which the insurer is subject. This procedure is important for all significant policy-coverage lines. Rating agencies typically consider a number of insurers vulnerable, and some underwriters may have large environmental exposures but capped equity resources. Many large commercial enterprises acquire insurance coverage from foreign companies or from subsidiaries of U.S. insurers domiciled in the Caribbean or other countries. The quality of insurance supervision in many foreign countries may not meet the standards expected in the United States.

TYPES OF RISKS

Business risks generally fall into three categories: (1) physical property damage, (2) liability resulting from product failure or unintended employee performance, and (3) loss of key personnel. Common property risks are fires or natural disasters such as storms and earthquakes, but acts of violence or terrorism can also be included in this category. Risk-management programs for property damage should consider not only the protection and replacement of the physical plant, but also the effects of business interruptions, loss of business assets, and reconstruction of records.

Insurance programs increasingly cover the consequences of the second category, product failure or unintended employee performance. These risks include the injury or death of employees, customers, and others; official misconduct; and individual and class-action lawsuits alleging mistreatment or the violation of laws or regulations. All aspects of a bank's operation are susceptible to liability risks. While property-loss levels can be estimated with relative confidence, jury awards for personal injury or product liability, and the related litigation costs, often exceed expectations. In addition, it can be difficult to identify potential sources of liability exposure.

The third category, personnel risk, concerns those exposures associated with the loss of key personnel through death, disability, retirement, or resignation, as well as threats to all employees and third parties arising out of crimes such as armed robbery and extortion. The consequences of personnel loss are often more pronounced in small and medium-sized banks that do not have the financial resources to support a broad level of management.

INSURANCE PROGRAM

Program Objectives

A bank's insurance program should match the objectives of its management, the director-approved risk guidelines, and its individual risk profile. Insurance is primarily the transfer of the financial effect of losses and should be considered as only a part of the broader risk-management process. In that sense, it is imperative that management understands the costs and benefits of the bank's insurance program.

Due to the fluid nature of the insurance market and insurance products, there is no standard program or contract structure. Rather, many different insurance policies, coverages, endorsements, limits, deductibles, and payment plans fit together to form an insurance program. Based on the size and scope of a bank's operations, broader or narrower coverage, higher or lower limits, and separate policies may be purchased. Insurance programs should be customized to the risks that each bank faces. If a bank is particularly susceptible to a specific risk, purchasing additional insurance for that risk may be prudent.

A policy's deductible size and coverages, and the limits purchased, determine how much risk the bank has retained. Likewise, the payment plan of an insurance policy greatly influences the amount of risk transferred. An insurance policy alone does not represent significant risk transfer if the payment plan includes reimbursement to the insurance company for all losses, usually subject to a maximum. These reimburse-

ment, loss-sensitive, or retrospectively rated plans can be viewed more as a risk-financing tool than as risk transfer. Management should understand and quantify the total "all-in" cost of these plans, as well as how these costs correspond with the risk guidelines approved by the directors.

Common Insurance-Policy Components and Concepts

There is a difference between "policy" and "coverage," but the two terms are often used interchangeably. The term "policy" usually refers to the actual insurance contract, while the term "coverage" refers to the types of risks to which the policy is designed to respond. For example, a directors' and officers' policy may include employment-practices liability (EPL) coverage. However, the bank may also purchase a separate EPL policy

An "endorsement" is a modification to a policy. Endorsements can be either a simple change in wording from the original contract or a more complex addition or deletion of a coverage section. To expand on the example above, EPL coverage is often endorsed onto a directors' and officers' policy. When an endorsement adds a coverage to a policy, it is often called a "rider."

The "limit of insurance" is the dollar amount of insurance protection purchased. Each policy has a different limit, and some may have separate limits for separate coverages provided under the same policy. Policies usually include a "per-occurrence" and an "aggregate" limit. The per-occurrence limit is the most the insurer will pay under the policy for any one insured event, while the policy aggregate is the most the insurer will pay in total, regardless of the number and size of insurable events.

"Deductibles" and "self-insured retentions (SIRs)" are the dollar amounts the bank must contribute to the loss before insurance applies.[1] They are effectively the same concept, with the difference being a deductible reduces the limits of insurance while a SIR does not. A deductible is included within or as part of the limits. A SIR is outside or in addition to the provided limits. For example, a $5 million policy limit with a $1 million deductible consists of $4 million of protection and the $1 million deductible. A $5 million policy limit with a $1 million SIR provides $5 million in protection after the $1 million dollar SIR is paid by the bank. As in any clause of an insurance contract, the terms can be negotiated so a deductible does not reduce the limits.

"Occurrence" and "claims made" are two separate types of coverage bases of policies that differ as to the period protected, when claims are recognized, and when the policies are "triggered" or respond. Under an occurrence, or "loss-sustained," form the amount and type of coverage (if any) for the loss event is based on the policy that was in force when the event took place or occurred, regardless of when a claim is submitted. Under a claims-made, or "discovery," policy, the insurance policy in force when the loss event was discovered and reported to the insurance company would apply, regardless of when the event causing the claim occurred. Both types of policies have provisions regarding prompt claims-reporting to insurers. However, claims-made policies are usually stricter and their coverage may be compromised by failing to report claims in a timely manner.

Self-Insurance or Alternative Risk Transfer

There are numerous nontraditional insurance programs that larger, more complex banking organizations employ. These programs include, but are not limited to, captive insurance companies, individual or group self-insurance, risk-retention groups, and purchasing groups. These alternative risk-transfer (ART) programs are complex, and they should include common bank policies and procedures. For example, the bank should have access to individuals with insurance expertise. Outside consultants, qualified insurance brokers, and bank directors or management with insurance expertise are an integral part of a successful ART program. The ART program should also incorporate stop-loss provisions and reinsurance coverage to cap the organization's exposure to severe claims or unexpected loss experience.

COMMON POLICIES AND COVERAGES

The following is not intended to be a compre-

1. An organization can maintain an unfunded reserve for loss-retention purposes.

hensive list of policies and coverages available, but rather a listing and description of those that banks most frequently purchase. The list is divided into three general types of insurance: liability, property, and life insurance. A fourth category is included for aircraft and aviation insurance, which consists of various types of property and liability coverage. While this last coverage category may be unnecessary for most banking organizations, for those institutions that do have exposure to risks associated with aircraft ownership, the risks may be exceptionally large.

Fidelity Insurance Bond

Liability insurance is sometimes called ''third-party insurance'' because three parties are involved in a liability loss: the insured, the insurance company, and the party (the claimant) who is injured or whose property is damaged by the insured. The insurance company pays the claimant on behalf of the insured if the insured is legally liable for the injury or damage. An insured's legal liability for injury is often the result of a negligent act, but there are other sources of liability. Several examples of liability insurance are discussed below.

Fidelity bond coverage provides reimbursement for loss from employee dishonesty; robbery; burglary; theft; forgery; mysterious disappearance; and, in specified instances, damage to offices or fixtures of the insured. Coverage applies to all banking locations except automated teller machines, for which coverage must be specifically added. All banks should obtain fidelity bond coverage that is appropriate for their business needs.

The most widely used form of fidelity bond is the Financial Institution Bond (FIB), Standard Form No. 24 (formerly named the bankers' blanket bond). Standard Form No. 24 is a claims-made, or discovery, form. The ''basic'' FIB has four insuring agreements or parts. Employee Dishonesty/Fidelity (Clause A) covers dishonest or fraudulent acts committed by employees. On-Premises (Clause B) covers losses from burglary, misplacement, or an unexplained disappearance that occurs on premises. In-Transit (Clause C) covers losses from burglary, misplacement, or an unexplained disappearance that occurs while the property is in transit. Counterfeit Currency (Clause F) covers losses from accepting counterfeit currency.

In addition to the basic four FIB insuring agreements, Forgery or Alteration (Clause D) and Securities (Clause E) may also appear on the standard form. (These coverages may not be a component of the most basic insurance program for a small bank.) Significant enhancements and additional coverages are often endorsed onto the FIB. Any misrepresentation, omission, concealment, or incorrect statement of material fact in the insurance application is grounds for recission of the fidelity bond by the underwriting insurance company.

When the bank under examination is a subsidiary of a bank holding company, and the holding company has purchased one fidelity bond to cover all affiliated banks, the examiner should determine that the policy is sufficient to cover the exposures of the subsidiary bank being examined. Examiners also should determine that any policy premiums the subsidiary bank pays to the parent holding company are not disproportionate to the bank's benefits from the group policy and that such premiums are consistent with the fair-market requirements of section 23B of the Federal Reserve Act. Split-limit coverage may reduce protection if a loss involves the collusion of subsidiary bank employees or other affiliates of a bank holding company.

Clause A: Fidelity (Employee Dishonesty)

Clause A covers losses resulting directly from dishonest or fraudulent acts an officer or employee commits, either acting alone or in collusion with others. The employee must have had a manifest intent to cause a loss to the financial institution, and the employee or another person or entity must obtain financial benefit from the dishonest or fraudulent act. Officers, attorneys retained by the bank, persons provided by an employment contractor, and nonemployee data processors who are performing services for the insured are typically all considered ''employees.'' If any of the loss results from loans, that part of the loss is covered only if the employee was in collusion with other parties to the transaction and the employee received a minimum financial-benefit amount, as specified in the policy. (''Financial benefit'' does not include any employee benefits earned in the normal course of employment, including salaries, commissions, fees, bonuses, promotions, awards, profit-sharing plans, or pensions.) Clause A should not prevent the recovery of losses from

employee dishonesty that are concealed by fictitious loans.

Clause B: On-Premises

Clause B covers losses of property (as defined in the bond) that occur on premises as a result of robbery, burglary, larceny, misplacement, theft, or a mysterious and unexplained disappearance. Under specified conditions, damage to offices and equipment may be covered under this clause, However, premises coverage should not be confused with standard fire or other types of property insurance.

Clause C: In-Transit

Clause C covers loss of property that is in transit. The property typically must be in the custody of (1) a natural person acting as a messenger for the insured, (2) a transportation company transporting the property in an armored motor vehicle, or (3) a transportation company transporting the property by means other than an armored motor vehicle. When an armored vehicle is not used by a transportation company, ‘‘property’’ is generally limited to records, certified securities, and negotiable instruments that are not payable to the bearer, are not endorsed, and have no restrictive endorsements. Some insuring agreements insure certain financial institution employees that carry cash.

Clause D: Forgery or Alteration

Clause D covers forgery, which is the signing of the name of another person or organization with the intent to deceive. Clause D also covers losses resulting from the alteration of any negotiable instrument. Evidences of debt, which the bank receives either over-the-counter or through clearings, are not usually covered. Fraudulent items received through an electronic funds transfer system are generally excluded.

Clause E: Securities

Clause E covers losses that result from a bank’s extending credit or assuming liability on the faith of original securities, documents, or written instruments that are forged, altered, lost, or stolen. These include but are not limited to a certificated security, a title, a deed or mortgage, a certificate of origin or title, an evidence of debt, a security agreement, an instruction to a Federal Reserve Bank, and a statement of uncertificated security of a Federal Reserve Bank. Coverage is included for certain counterfeit securities and instruments. The bank must have acted in good faith and had actual physical possession of the original instrument.

Clause F: Counterfeit Currency

Clause F provides coverage for losses resulting from the receipt of counterfeit money. The coverage is counterfeit money of the United States, Canada, or any other country where the insured maintains a branch office.

Common FIB Extensions, Riders, or Endorsements

Fidelity bond protection can be extended by purchasing additional coverage through extensions, riders, and endorsements. If a bank has significant risk exposures in certain areas, these additional protections should be considered. The most common of these protections are listed below.

Extortion/Threats to Persons or Property

The extortion/threats to persons or property rider insures against loss of property that is surrendered away from a banking office as the result of a threat to do bodily harm to a director, trustee, employee, or relative, or of threats to damage banking premises or property. While a bank may add this coverage with a rider to its FIB, many banks purchase a separate, more comprehensive policy or endorse this coverage onto the directors’ and officers’ policy.

Trading Losses

The trading-loss rider amends the FIB exclusion by providing coverage for trading losses resulting directly from employee dishonesty.

Automated Teller Machines

The automated teller machine (ATM) rider cov-

ers losses of money from, or damage to, an unattended ATM that results from robbery, burglary, or theft.

Electronic or Computer Systems

The electronic or computer-systems rider covers direct losses caused by fraudulent funds transfers originated through the bank's computer systems. The fraud may be caused by a dishonest employee, customer, or third party.

Unauthorized Signatures

The unauthorized-signature rider covers losses resulting from a bank's acceptance, cashing, or payment of any negotiable instrument or withdrawal order that bears an unauthorized signature. An ''unauthorized signature'' is not forged, but is the signature of an individual who is not an authorized signatory on the account.

Fraudulent Mortgages

The fraudulent-mortgages rider insures against loan losses that result from a bank's accepting or acting on mortgages or deeds of trust that have defective signatures. ''Defective signatures'' are those obtained through fraud or trickery or under false pretenses.

Counterfeit Checks

The counterfeit-check rider insures against loss from counterfeit checks and other negotiable instruments. The coverage applies whether or not the counterfeit instruments are forged.

Service Contractors

The service-contractor rider covers loss resulting from fraudulent or dishonest acts committed by a servicing contractor. A ''servicing contractor'' services real estate and home-improvement mortgages, as well as tax and insurance escrow accounts; manages real property; or provides other related services. The coverage extends to losses resulting from the contractor's failure to forward collected funds to the bank when the servicing contractor has committed to do so.

Money-Order Issuer's

With a money-order-issuer's rider, coverage is expanded to authorized third parties that issue registered checks or personal money orders on behalf of the insured.

Liability Insurance

Electronic and Computer Crimes

To broaden the electronic and computer-systems rider that is normally attached to the FIB, an additional electronic and computer-crime rider may be purchased. This rider is a ''companion policy'' that covers losses the bank may incur from having (1) transferred, paid, or delivered any funds or property; (2) established any credit; or (3) debited any account or given value as a direct result of fraudulent input of electronic data or computer instructions into the insured's computer. These losses may result from someone's unauthorized access to a terminal or the bank's communications lines, or from the fraudulent preparation of tapes or computer programs. Under this rider, coverage may include electronic funds transfer systems, the bank's proprietary systems, and voice instructions given over the telephone. Losses caused by software programmers and consultants, ATM systems, computer viruses, software piracy, computer extortion, and facsimiles may also be covered.

Excess Bank Employee Dishonesty Bond

The excess bank employee dishonesty bond adds limits over and above the FIB. Often an FIB cannot be purchased with limits that are large enough to satisfy the risk-transfer needs of larger banks. When this occurs, the bank may purchase an excess bond that would respond if a claim is larger than the per-occurrence limits on the FIB or if the aggregate limit of the FIB has been exhausted. The most common form of this coverage is the excess bank employee dishonesty blanket bond, Standard Form No. 28.

Combination Safe Depository

Combination safe depository insurance consists of two coverage sections that can be purchased

together or separately. Coverage (A) applies to losses when the bank is legally obligated to pay for loss of a customer's property held in safe deposit boxes (including loss from damage or destruction). Coverage (B) generally covers loss, damage, or destruction of property in customers' safe deposit boxes, whether or not the bank is legally liable, when the loss results from an activity other than employee dishonesty, such as robbery or burglary.

Directors' and Officers' Liability

Directors' and officers' (D&O) liability insurance usually has three coverage parts: Side A, Side B, and Entity Securities Coverage (C). Side A covers the directors and officers individually for alleged wrongful acts. Side B reimburses the bank for money it has paid to or on behalf of its directors and officers to indemnify them for damages they may be liable for as a result of alleged wrongful acts. Entity Securities Coverage protects the corporation against securities claims. Subject to many exclusions and definitions, a "wrongful act" means any actual or alleged act, error, omission, misstatement, misleading statement, neglect, or breach of duty. D&O policies are primarily written on a claims-made basis. Larger banks will purchase excess D&O coverage. Like the FIB, there are numerous coverages or enhancements that can be endorsed onto a D&O policy.

Entity errors and omissions. The entity errors and omissions (E&O) insurance rider extends coverage to the financial institution as an entity for wrongful acts. A separate, more robust E&O policy may also be purchased. The separate policy is commonly referred to as bankers' professional liability.

Fiduciary liability and ERISA errors and omissions. Fiduciary liability (or fiduciary errors and omissions) extends insurance coverage for management of the bank's own employee pension or profit-sharing plans. A separate, more robust fiduciary policy may be purchased to expand further the coverage of the bank's management of its own plans. Without this additional special endorsement, neither the fiduciary errors and omissions nor the bank's directors' and officers' liability insurance will cover liability arising under the Employee Retirement Income Security Act of 1974 (ERISA). For protection against exposure arising from a breach of fiduciary duty under ERISA, a special ERISA errors and omissions endorsement is required (also called fiduciary or employee benefit plan liability). In addition to bank trust departments, banks whose only fiduciary responsibilities relate to their employee benefit plan should consider this coverage. A related specialized coverage called IRA/Keogh errors and omissions is also available.

For properties held or managed by a bank's trust department, a master or comprehensive policy is often obtained instead of individual policies. A master policy protects the trust-account properties from fire or other loss and insures the accounts and the bank against third-party liability in connection with the properties. The master policy does not usually cover claims by trust customers against the bank for negligence, errors, or violations resulting in loss to fiduciary accounts. However, separate fiduciary (or trust department) errors and omissions policies incorporate these areas.

Trust Errors and Omissions

Trust errors and omissions insurance provides coverage for wrongful acts while the bank is acting as trustee, guardian, conservator, or administrator. This is a claims-made policy that can be endorsed onto the D&O policy.

Employment-Practices Liability

Employment-practices liability (EPL) insurance provides coverage for an entity against employee claims of wrongful termination, discrimination, sexual harassment or "wrongful employment acts." This is usually a claims-made policy that can be endorsed onto the D&O policy.

Bankers' Professional Liability

Bankers' professional liability (BPL-E&O) provides coverage for claims resulting from any actual or alleged wrongful acts, errors, or omissions bank employees commit in the performance of professional duties. Coverage can be broadened to include securities E&O, insurance agent E&O, brokerage service E&O, and notary E&O.

Mortgage Impairment

Mortgage-impairment insurance coverage protects the bank's interest, as mortgagee, from loss when contractually required insurance on real property held as collateral has inadvertently not been obtained. Upon discovery of the lack of required coverage, the bank has a limited time to either induce the borrower to obtain the required insurance or to place the insurance on its own.

Mortgage Errors and Omissions

Mortgage errors and omissions insurance, a broader version of mortgage-impairment coverage, provides coverage for direct damage and E&O losses to either the bank or the borrower. Mortgage E&O coverage also applies to the bank's mishandling of real estate taxes, life and disability insurance, and escrowed insurance premiums. Claims must result in a loss to the mortgaged property.

Commercial General Liability

Commercial general liability (CGL) insurance protects against claims of bodily injury or property damage for which the business may be liable and which may arise from the bank's premises, operations, and products. In addition to bodily injury and property damage, CGL can include liability coverage for various other offenses that might give rise to claims, such as libel, slander, false arrest, and advertising injury. A CGL policy can be underwritten on either an occurrence or a claims-made basis.

Workers' Compensation and Employers' Liability

Workers' compensation insurance covers injuries or deaths of employees caused by accidents in the course of employment. Workers' compensation insurance consists of two basic coverage parts: statutory benefits and employers' liability (EL). The two are mutually exclusive remedies to an employee injured on the job. EL protects a company from a lawsuit filed by an employee, while statutory benefits coverage provides medical care and long-term disability, death, or other benefits. State laws govern these provisions, so the provisions differ from state to state. The statutory coverage of workers' compensation is a no-fault system intended to benefit both the injured employee and the employer.

Automobile Liability and Physical Damage

Automobile liability insurance provides third-party liability protection for bodily injury or property damage resulting from accidents that involve the bank's vehicles. First-party coverage for damage to the vehicles is also provided. This coverage should be extended to include—

- nonowned and hired coverage, if employees use personal autos or rent autos while on bank business;
- coverage for autos that have been repossessed; and
- garage-keeper's liability, if the bank rents its parking facilities to customers or the public.

Umbrella and Excess Liability

Umbrella and excess liability insurance offers additional liability limits in excess of the coverage limits of any policy over which it "attaches" or becomes effective. Basic umbrella coverage attaches to CGL and automobile insurance and to the employers' liability section of workers' compensation policies. An excess liability policy attaches over an umbrella policy. More complex insurance programs may include both umbrella and excess liability policies that attach over the D&O, E&O, EPL, or other insurance.

Property Insurance

Several types of insurance coverage are available to help banks recover from property damage. Some of the more common types of property coverages are briefly described below.

Broad Form Property Insurance

Property insurance insures against the loss of or damage to real and personal property. The loss or damage may be caused by perils such as fire,

theft, windstorm, hail, explosion, riot, aircraft, motor vehicles, vandalism, malicious mischief, riot and civil commotion, and smoke.

Fire

Fire insurance covers all losses directly attributed to fire, including damage from smoke or water and chemicals used to extinguish the fire. Additional fire damage for the building contents may be included, but often is written in combination with the policy on the building and permanent fixtures. Most fire insurance policies contain "co-insurance" clauses, meaning that insurance coverage must be maintained at a fixed proportion of the replacement value of the building. If a bank fails to maintain the required relationship of protection, all losses will be reimbursed at the ratio of the amount of the insurance carried to the amount required, applied to the value of the building at the time of the loss. When determining insurable value for fire insurance purposes, the basis typically is the cost of replacing the property with a similar kind or quality at the time of loss. Different types of values, however, may be included in policies, and care should be taken to ensure that the bank is calculating the correct value for its needs.

Business Personal Property

Traditionally known as "contents" insurance, business personal property insurance affords insurance protection coverage for the furniture, fixtures, equipment, machinery, merchandise, materials, and all other personal property owned by the bank and used in its business.

Blanket Coverage

Blanket insurance covers, in a single contract, either multiple types of property at a single location or one or more types of property at multiple locations.

Builder's Risk

Builder's-risk insurance is commercial property coverage specifically for buildings that are in the course of construction.

Business Interruption

Business-interruption insurance indemnifies the insured against losses arising from its inability to continue normal operations and functions of the business. Coverage is triggered by the total or partial suspension of business operations due to the loss of, loss of use of, or damage to all or part of the bank's buildings, plant machinery, equipment, or other personal property, when the loss is the result of a covered cause.

Contingent business-interruption insurance is also available to cover the bank's loss of earnings caused by a loss to another business that is one of its major suppliers or customers. This insurance is also known as "business income from dependent properties."

Crimes

Crime insurance covers money, securities, merchandise, and other property from various criminal causes of loss, such as burglary, robbery, theft, and employee dishonesty.

Data Processing

Data processing insurance coverage provides loss protection if data processing systems break down. This insurance also covers the additional expense incurred in making the system operational again.

Difference in Conditions

A difference-in-conditions (DIC) insurance contract is a separate coverage that expands or supplements property insurance that was written on a named-perils basis. A DIC policy will cover the property on an all-risk basis, subject to certain exclusions.

Ocean and Inland Marine

Ocean marine insurance covers ships and their cargo against such causes as fire, lightning, and "perils of the seas." These include high winds, rough waters, running aground, and collision with other ships or objects.

Inland marine insurance was originally developed to provide coverage for losses to

cargo transported over land. It now covers limited types of property in addition to goods in transit.

Valuable Papers and Destruction of Records

Valuable-papers and destruction-of-records insurance coverage is for the physical loss or damage to valuable papers and records of the insured. The coverage includes practically all types of printed documents or records except money.

Accounts Receivable

Accounts-receivable insurance covers losses that occur when an insured is unable to collect outstanding accounts because of damage to or destruction of the accounts-receivable records that was caused from a peril covered in the policy.

Cash Letters

Cash-letter insurance covers the costs for reproducing cash-letter items and items that remain uncollectible after a specified period of time. Generally, these policies do not cover losses due to dishonest acts of employees.

First-Class, Certified, and Registered Mail

The insurance coverage for first-class, certified, and registered mail provides protection on the shipment of property sent through the mail, as well as during transit by messenger or carrier to and from the post office. The insurance is principally used to cover registered mail in excess of the maximum $25,000 insurance provided by the U.S. Postal Service.

Commercial Multiple Peril

Commercial multiple peril insurance encompasses a range of insurance coverages, including property and liability. Small institutions may purchase this package policy when stand-alone polices are excessive or inefficient.

Life Insurance

Common types of life insurance policies purchased by banks are described below.

Key Person

When the death of a bank officer, or key person, would be of such consequence to the bank as to give it an insurable interest, key-person life insurance would insure the bank on the life of this individual.

Split-Dollar

In split-dollar life insurance, the purchaser of the policy pays at least part of the insurance premiums and is entitled to only a portion of the cash surrender value, death benefit, or both. See SR-93-37 (“Split-Dollar Life Insurance,” June 18, 1993) and its attachments for further discussion of the Federal Reserve’s position on these arrangements between bank holding companies and their subsidiary banks.

Bank-Owned

Bank-owned life insurance consists of tax-advantaged insurance policies that are purchased to cover the lives of bank officers and other highly compensated employees. The policies may be used as a funding mechanism for employee pension and benefit plans. The bank is the owner and beneficiary of the policy, and the cash value of the policy is considered an asset of the bank.

Aircraft or Aviation Insurance

Although aviation-liability exposures are frequently overlooked in the myriad of other financial institution exposures, they have tremendous potential for large catastrophic losses and must be addressed by senior risk-management executives at all financial institutions. Often hidden or obscure, aviation liability ranges from the more typical owned and nonowned liability and physical-damage exposures to the more exotic exposures from hangar-keepers, aviation products, and airport or heliport premises. In view of the specialized nature of aviation exposures, it is

important that the bank deal with knowledgeable and experienced agents or brokers and underwriters in developing its aviation insurance program. While exposure categories overlap significantly, the following summary highlights the key areas of concern to most financial institutions.

Aviation Liability

Aviation liability insurance can be written to include aviation-products liability, all owned or nonowned exposures, and passenger liability. A bank's umbrella liability insurance program should also apply over the aviation policy's limit.

Nonowned Exposures

While many banks do not feel the need for aviation insurance because they do not own an aircraft, they may overlook liability exposures from nonowned aircraft and may, in fact, need this coverage. For example, an employee may use a personal aircraft on bank business, or lease or rent an aircraft to ferry customers or employees to a distant meeting. Financing or leasing an aircraft could create a nonowned exposure, even though the aircraft is not under bank control.

Most aviation-underwriting markets have programs available to meet the above exposures. However, additional exposures may require special coverage. Banks should consider the following situations:

- If the bank repairs and maintains the aircraft, it may incur a products-liability exposure after control is relinquished to others, such as when the aircraft is sold.
- If the bank finances aircraft, maintaining only a security interest, it becomes an owner when it repossesses the aircraft. In this case, there could be a definite need for both liability and physical-damage coverage. The coverage may be written at the time of repossession or negotiated in advance of the need for it. The bank should not attempt to continue coverage for its exposure under the borrower's policy.

All-Risk Physical Damage

To protect the bank's security interest in an aircraft hull, borrowers should be required to maintain full-value, all-risk physical-damage insurance (both ground-risk and in-flight coverage) in favor of the bank. However, a number of warranties in aircraft insurance policies could void the contract, so bankers are further advised to require that a borrower's hull insurance policy contain a breach-of-warranty endorsement to protect the bank if the borrower or owner violates provisions of the policy. The underwriter should agree to give the bank at least 30 days' advance notice of any change in the policy. Depending on the use of the aircraft, special consideration should be given to the territorial limits of coverage, as well as to confiscation protection. Since breach-of-warranty endorsements, like aircraft insurance policies, are far from standard, it is important that the bank understand and agree with the underwriter's language. It is particularly appropriate to review the consequences of potential recovery to the lien holder if the aircraft is damaged while a delinquency exists on the note.

Bank as Lessor

If the bank's security interest is that of the lessor, aviation liability insurance should be carried by the bank as lessor and also by the customer as lessee. In certain cases, it may be appropriate to require the lessee, through his or her underwriter, to provide the equivalent of the breach-of-warranty endorsement to the liability program and physical-damage coverage. The bank may also consider obtaining contingent lessor's liability.

Airport Premises and Hangar-Keepers

Airport-premises and hangar-keeper's insurance apply if the bank repossesses real estate on which an airport facility exists and continues to operate, or if the bank permits use of the facility pending further sale. In either case, the bank may assume liability exposures associated with the control tower, as well as airport-premises liability. Both the bank's comprehensive general liability and aviation liability programs should be reviewed for proper coverage.

If the bank owns or operates a hangar for its aircraft and attempts to share the burden of costs with others by renting aircraft space, it can pick up exposure to hangar-keeper's liability, unless

the contract is properly worded. Appropriate consideration should be given to hold-harmless indemnification clauses, any regular or special insurance requirements, and waivers of subrogation.

Accidental Death and Dismemberment and Travel

Accidental death and dismemberment and travel insurance is another aspect of aviation insurance that banking institutions should consider. Many insurance programs for accidental death and dismemberment and corporate business travel accidents exclude coverage in corporate-owned, -leased, or -hired aircraft. Banks need to review the language of these policies carefully to be certain that they provide necessary and adequate coverages for the use of such aircraft.

RECORDKEEPING

The diversity of available insurance policies and their coverages emphasize the need for banks to maintain a concise, easily referenced schedule of their insurance coverage, referred to as the "schedule of insurance." These records should include the following information:

- insurance coverages provided, with major exclusions detailed
- the underwriter
- deductible amounts
- upper limits on policies
- terms of the policies
- dates that premiums are due
- premium amounts
- claim-reporting procedures

In preparation for policy renewal, the bank's risk manager and insurance broker organize much of the bank's relevant insurance data into a "submission." The submission may include—

- historical, current, and forecasted exposure information, such as sales, number and type of employees, property characteristics and values, and number and type of autos;
- loss and claim history by line of insurance, including detailed information on large claims, loss development, and litigation;
- information on company risk-management policies and financials; and
- specifications on desired coverages, terms and conditions, limits, deductibles, and payment plans.

The submission is delivered to the insurance company underwriter and forms the basis for determining premiums, rates, limits, and the program structure. The information may give the examiner a sense of why premiums and coverages change from year to year and whether purchased limits are sufficient.

Banks should retain the original policies and supporting documents for appropriate time periods. Records of losses should also be maintained, regardless of whether the bank was reimbursed. This information indicates areas where internal controls may need to be improved and is useful in measuring the level of risk exposure in a particular area.

1. To determine whether insurance is effectively integrated into the operational-risk-management program, and whether the insurance is appropriate, in light of the institution's internal-control environment.
2. To determine if insurance coverage adequately protects against significant or catastrophic loss.
3. To determine if recordkeeping practices are sufficient to enable effective risk and insurance management.
4. To ascertain if, and ensure that, the risk manager has initiated corrective action when policies, practices, procedures, or internal controls are deficient or when violations of banking laws and regulations have been noted.

1. If selected for implementation, complete or update the ''Bank Risk and Insurance Management'' section of the internal control questionnaire.
2. Test for compliance with policies, practices, procedures, and internal controls in conjunction with performing the remaining examination procedures. From the examiner who is assigned to ''internal control,'' obtain a listing of any deficiencies noted in the latest review conducted by internal or external auditors and risk managers. Determine if appropriate corrections have been made.
3. Determine if the bank has designated a qualified risk manager, with expertise in insurance programs, to be responsible for loss control. If not, determine which officer handles the risk- and insurance-management function and whether external consultants are employed in designing the insurance program.
4. Obtain the bank's schedule of insurance policies in force and the renewal submissions. If the bank does not maintain a schedule, request that the bank complete a schedule of existing insurance coverage.
   a. Determine whether there have been any material changes in insurance coverage, limits, or deductibles since the last examination and the reasons for such changes. Do the changes reflect—
      - revised business strategies, the bank structure, operating processes, or technology systems that affect insurable risks, and
      - shifts to self-insurance or co-insurance or a change in insurance carriers?
   b. If there have been material changes, determine how they are being managed.
5. Using the bank-prepared summary of insurance coverage, determine that coverage conforms to the guidelines for maximum loss exposure, as established by the board of directors.
   a. Determine whether the use of insurance is in accordance with board-approved risk-management policies and guidelines.
   b. If the bank self-insures, determine what methods are used for this purpose; how the value of self-insurance is quantified; and how ''premiums'' are accounted for, funded, allocated, and tracked.
6. Determine whether insurance coverage provides adequate protection for the bank. The quality of internal controls and the audit function must be considered when making this assessment.
   a. Determine whether the bank manages its insurance coverage as an element of the operational-risk-management program.
   b. Determine whether the insurance program is managed on a corporate-wide basis or within each business unit.
   c. Identify any products, processes, or systems that the bank is not able to obtain insurance coverage for and determine how the associated risk is being managed.
   d. Determine whether the bank maintains a database of operational-loss events, the comprehensiveness of the database, and the claims history of operational losses.
   e. Review the due-diligence process used to assess the qualifications of providers of insurance coverage, including primary reinsurers.
7. If the bank's fidelity insurance has lapsed, determine that the appropriate Federal Reserve Bank has been notified.
8. Determine that the bank has adequate procedures to ensure that—
   a. reports of losses are filed with the bonding company pursuant to policy provisions,
   b. premiums are paid before policy expiration dates,
   c. policies are renewed without a lapse of coverage at expiration dates, and
   d. material changes in exposures are reported to the bank's insurance agent or broker and result in appropriate insurance-policy endorsements.

If the procedures are deficient, verify that reports have been filed as required and premiums have been paid.

9. Review any significant financial institution bond claims that were filed since the last examination to determine—

a. any adverse effect on the bank's condition,
b. whether the incident (or incidents) reflects any deficiencies with respect to internal controls and procedures, and
c. whether management has taken appropriate steps to correct any deficiencies and made appropriate reports to the board of directors.

10. Prepare, in appropriate report form, and discuss with appropriate officers—
    a. recommended corrective action when policies, practices, procedures, or internal controls are deficient;
    b. recommended improvements in the risk-management program that relate to insurance;
    c. important areas in which insurance coverage is either nonexistent or inadequate in view of current circumstances; and
    d. any other deficiencies noted.
11. Update the workpapers with any information that will facilitate future examinations.

Review the bank's internal controls, policies, practices, and procedures for its own insurance coverage. The bank's risk-management system should be documented completely and concisely and should include, where appropriate, the risk-assessment matrix, a narrative description, flowcharts, the schedule of insurance coverage, policy forms, renewal submissions, and other pertinent information.

BANK RISK AND INSURANCE MANAGEMENT

1. Does the bank have established insurance guidelines that provide for—
   a. a reasonably frequent, and at least annual, determination of risks the bank assumes or transfers, including high-dollar and low-probability events?
   b. limits as to the amount of risk that may be retained or self-insured?
   c. periodic appraisals of major fixed assets to be insured?
   d. a credit or financial analysis of the insurance companies who have issued policies to the bank?
2. Does the bank have a risk manager who is responsible for assessing and developing controls to deal with the consolidated risks of the institution?
3. Is the bank's insurance program managed as an element of its overall operational-risk-management program; that is, are insurance coverages reviewed and coordinated by the person handling the operational-risk-management function?
4. Does the bank use the services of a professionally knowledgeable insurance agent, broker, direct writer, or consultant to assist in selecting and providing advice on alternative means of providing insurance coverage?
5. Does the bank's security officer coordinate his or her activities with the person responsible for handling the operational-risk-management function?
6. Does the bank maintain a concise, easily referenced schedule of existing insurance coverage?
7. Does the bank maintain records, by type of risk, to facilitate an analysis of the bank's experience in costs, claims, losses, and settlements under the various insurance policies in force?
8. Is a complete schedule of insurance coverage presented to the board of directors at least annually for review and approval? Does the schedule include the respective insurance premiums (net costs), claims, and loss experience, and is this information reviewed as part of this process?

CONCLUSION

1. Is the foregoing information an adequate basis for evaluating internal control; that is, there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
2. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

State member banks may purchase bank-owned life insurance (BOLI) as principal if such purchases are permitted for national banks and permitted under state law. The legal authority and guidance for acquiring permissible BOLI and for engaging in insurance activities is discussed within the following interagency statement. When such insurance purchases or insurance activities are not permissible for national banks, a determination of permissibility depends on a decision of the FDIC (1) that the investment or activity would not pose any significant risk to the insurance fund and (2) that the bank continues to comply with the required capital standards.

The bank supervisory agencies have concerns that some banks have committed a significant amount of capital to BOLI without having an adequate understanding or a proper assessment of the full array of risks it poses—especially risks that are difficult to measure, such as liquidity, transaction/operational, reputation, and compliance/legal risks. Banks are therefore expected to implement appropriate risk-management processes, including meaningful risk limits, before implementing or adding to a BOLI program. The following interagency guidance was developed for banks and savings associations (institutions) and examination staff to help ensure that risk-management practices for BOLI are consistent with safe and sound business practices. The interagency statement was issued on December 7, 2004.

INTERAGENCY STATEMENT ON THE PURCHASE AND RISK MANAGEMENT OF LIFE INSURANCE

This interagency statement[1] provides general guidance for banks and savings associations (institutions) regarding supervisory expectations for the purchase of and risk management for BOLI. Guidance is also provided for split-dollar arrangements and the use of life insurance as security for loans. The agencies are providing this guidance to help ensure that institutions' risk-management processes for BOLI are consistent with safe and sound banking practices. Among the safe and sound banking practices discussed in this statement are (1) the need for senior management and board oversight of BOLI, including both a thorough pre-purchase analysis of risks and rewards and post-purchase risk assessment and (2) the permissibility of BOLI purchases and holdings, as well as their risks and associated safety-and-soundness considerations. The statement's appendix [titled appendix A for this section of the manual] contains a discussion of insurance types and the purposes for which institutions commonly purchase life insurance, as well as a glossary of BOLI-related terminology [titled appendix B for this section].

The statement's guidance for the pre-purchase analysis of life insurance applies to all BOLI contracts entered into after December 7, 2004. The guidance concerning the ongoing risk management of BOLI subsequent to its purchase applies to all holdings of life insurance regardless of when purchased. Institutions that purchase life insurance after December 7, 2004, that are not in compliance with this guidance may be subject to supervisory action. Institutions that entered into BOLI contracts before this date will be evaluated according to each agency's pre-purchase guidance in effect at that time.

Compliance with the supervisory guidance in this statement regarding permissible uses for insurance (e.g., recovery of the costs of providing benefits) does not determine whether the policy satisfies state insurable interest requirements.

Legal Authority

National banks may purchase and hold certain types of life insurance under 12 USC 24 (Seventh), which provides that national banks may exercise "all such incidental powers as shall be necessary to carry on the business of banking." Federal savings associations also may purchase and hold certain types of life insurance incidental to the express powers granted under the Home Owners' Loan Act. The OCC and OTS have delineated the scope of these authorities through various interpretations addressing the

1. Adopted by the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) (the agencies).

permissible use of life insurance by national banks and federal savings associations.

Under these authorities, national banks and federal savings associations may purchase life insurance in connection with employee compensation and benefit plans, key-person insurance, insurance to recover the cost of providing pre- and post-retirement employee benefits, insurance on borrowers, and insurance taken as security for loans. The OCC and OTS may approve other uses on a case-by-case basis.

National banks and federal savings associations may *not* purchase life insurance—

- for speculation;
- to provide funds to acquire shares of stock from the estate of a major shareholder upon the shareholder's death, for the further purpose of controlling the distribution of ownership in the institution;
- as a means of providing estate-planning benefits for insiders, unless the benefit is a part of a reasonable compensation package; or
- to generate funds for normal operating expenses other than employee compensation and benefits.

National banks and federal savings associations may not hold life insurance in excess of their risk of loss or cost to be recovered. For example, once an individual no longer qualifies as a key person because of retirement, resignation, discharge, change of responsibilities, or for any other reason, the risk of loss has been eliminated. Therefore, national banks and federal savings associations may be required to surrender or otherwise dispose of key-person life insurance held on an individual who is no longer a key person. Typically, term or declining term insurance is the most appropriate form of life insurance for key-person protection.

National banks and federal savings associations may hold equity-linked variable life insurance policies (that is, insurance policies with a return tied to the performance of a portfolio of equity securities held in a separate account[2] of the insurance company) only for the purpose of economically hedging their equity-linked obligations under employee benefit plans. As discussed more fully in the section on "Price Risk," for equity-linked variable life insurance holdings to be permissible, the national bank or federal savings association must demonstrate that—

- it has a specific, equity-linked obligation; and
- both at the inception of the hedge and on an ongoing basis, changes in the value of the equity-linked variable life insurance policy are highly correlated with changes in the value of the equity-linked obligation.

If a national bank or federal savings association does not meet these requirements, the equity-linked variable life insurance holdings are not permissible. The use of equity-linked variable life insurance holdings as a long-term hedge against general benefit costs is not permissible because the life insurance is not hedging a specific equity-linked liability and does not meet the "highly correlated" requirement.

As a general matter, the ability of state-chartered banks to purchase insurance (including equity-linked variable life insurance) is governed by state law. In some instances, state laws permit state-chartered banks to engage in activities (including making investments) that

2. A separate account is a design feature that is generally available to purchasers of whole life or universal life whereby the policyholder's cash surrender value is supported by assets segregated from the general assets of the carrier. Under such an arrangement, the policyholder neither owns the underlying separate account nor controls investment decisions (e.g., timing of investments or credit selection) in the underlying separate account that is created by the insurance carrier on its behalf. Nevertheless, the policyholder assumes all investment and price risk.

go beyond the authority of a national bank. The Federal Deposit Insurance Act (section 24) generally requires insured state-chartered banks to obtain the FDIC's consent before engaging as principal in activities (including making investments) that are not permissible for a national bank. Similarly, the Federal Deposit Insurance Act (section 28) generally requires a state-chartered savings association to obtain the FDIC's consent prior to engaging as principal in activities (including making investments) that are not permissible for a federal savings association. While insured state-chartered banks and state savings associations may seek the FDIC's consent to make purchases of life insurance that would not be within the authority of a national bank or federal savings association, such banks and savings associations should be aware that the FDIC will not grant permission to make life insurance purchases if the FDIC determines that doing so would present a significant risk to the deposit insurance fund or that engaging in such purchases is inconsistent with the purposes of federal deposit insurance.

Accounting Considerations

Institutions should follow generally accepted accounting principles (GAAP) applicable to life insurance for financial and regulatory reporting purposes. Financial Accounting Standards Board (FASB) Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance" (TB 85-4), discusses how to account for holdings of life insurance. Under TB 85-4, only the amount that could be realized under an insurance contract as of the balance-sheet date (that is, the CSV reported to the institution by the carrier, less any applicable surrender charges not reflected by the insurance carrier in the reported CSV) is reported as an asset. The guidance set forth in TB 85-4 concerning the carrying value of insurance on the balance sheet is generally appropriate for all forms of BOLI.

An institution may purchase multiple permanent insurance policies from the same insurance carrier with each policy having its own surrender charges. In some cases, the insurance carrier will issue a rider or other contractual provision stating that it will waive the surrender charges if all of the policies are surrendered at the same time. Because it is not known at any balance-sheet date whether one or more of the policies will be surrendered before the deaths of those insured, the possibility that the institution will surrender all of these policies simultaneously and avoid the surrender charges is a gain contingency. Under FASB Statement No. 5, "Accounting for Contingencies," "[c]ontingencies that might result in gains usually are not reflected in the accounts since to do so might be to recognize revenue prior to its realization." Accordingly, an institution should report each of the insurance policies on its balance sheet at the policy's CSV reported by the insurance carrier, less any applicable surrender charges not reflected in the reported CSV, without regard to the existence of the rider.

In accordance with the instructions for Consolidated Reports of Condition and Income and Thrift Financial Reports, an institution should report the carrying value of its BOLI holdings as an "other asset" and the earnings on these holdings should be reported as "other noninterest income."

The agencies have seen a number of cases in which institutions have failed to account properly for a type of deferred compensation agreement, commonly referred to as a revenue-neutral plan or an indexed retirement plan. The accounting for such plans is separate and distinct from the accounting for BOLI. However, because many institutions buy BOLI to help offset the cost of providing such deferred compensation, the agencies have issued guidance addressing the accounting requirements for both deferred compensation agreements and BOLI. See the Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance, dated February 11, 2004, for a complete description, including examples, of the appropriate accounting treatment.

Supervisory Guidance on BOLI

Before entering into a BOLI contract, institutions should have a comprehensive risk-management process for purchasing and holding BOLI. A prudent risk-management process includes—

- effective senior management and board oversight;
- comprehensive policies and procedures, including appropriate limits;

- a thorough pre-purchase analysis of BOLI products; and
- an effective ongoing system of risk assessment, management, monitoring, and internal control processes, including appropriate internal audit and compliance frameworks.

The risks associated with temporary (term) insurance are significantly less than those arising from holdings of permanent insurance. Accordingly, the risk-management process for temporary insurance may take this difference into account and need not be as extensive as the risk-management process for permanent insurance.

Senior Management and Board Oversight

The safe and sound use of BOLI depends on effective senior management and board oversight. Regardless of an institution's financial capacity and risk profile, the board must understand the complex risk characteristics of the institution's insurance holdings and the role this asset is intended to play in the institution's overall business strategy. Although the board may delegate decision-making authority related to purchases of BOLI to senior management, the board remains ultimately responsible for ensuring that the purchase and holding of BOLI is consistent with safe and sound banking practices.

An institution holding life insurance in a manner inconsistent with safe and sound banking practices is subject to supervisory action. Where ineffective controls over BOLI risks exist, or the exposure poses a safety-and-soundness concern, the appropriate agency may take supervisory action against the institution, including requiring the institution to divest affected policies, irrespective of potential tax consequences.

Policies and Procedures

Consistent with prudent risk-management practices, each institution should establish internal policies and procedures governing its BOLI holdings, including guidelines that limit the aggregate CSV of policies from any one insurance company as well as the aggregate CSV of policies from all insurance companies. When establishing these internal CSV limits, an institution should consider its legal lending limit, the capital concentration threshold, and any applicable state restrictions on BOLI holdings.[3] In this regard, given the liquidity, transaction/operational, reputation, and compliance/legal risks associated with BOLI, it is generally not prudent for an institution to hold BOLI with an aggregate CSV that exceeds 25 percent of the institution's capital as measured in accordance with the relevant agency's concentration guidelines.[4] Therefore, the agencies expect an institution that plans to acquire BOLI in an amount that results in an aggregate CSV in excess of 25 percent of capital, or any lower internal limit, to gain prior approval from its board of directors or the appropriate board committee. The agencies particularly expect management to justify that any increase in BOLI resulting in an aggregate CSV above 25 percent of capital does not constitute an imprudent capital concentration. An institution holding BOLI in an amount that approaches or exceeds the 25 percent of capital concentration threshold can expect examiners to more closely scrutinize the risk-management policies and controls associated with the BOLI assets and, where deficient, to require corrective action.

When seeking the board's approval to purchase or increase BOLI, management should inform the board members of the existence of this interagency statement, remind them of the illiquid nature of the insurance asset, advise them of the potential adverse financial impact of early surrender, and identify any other significant risks associated with BOLI. Such risks might include, but are not limited to, the costs associated with changing carriers in the event of a decline in the carrier's creditworthiness and the potential for noncompliance with state insurable interest requirements and federal tax law.

3. In July 1999, the OTS adopted a policy that savings associations may not invest more than 25 percent of their total capital in BOLI without first notifying and obtaining authorization from their OTS Regional Office. In order to maintain strong and effective communications with institutions under its supervision, the OTS retains this policy. The other agencies may also institute approval or notification requirements.

4. Each agency's definition of a concentration differs slightly. Institutions should refer to the definition provided by their supervisory agency when measuring the CSV of BOLI as a percentage of capital: OCC Bulletin 95-7 for national banks; FRB *Commercial Bank Examination Manual,* section 2050.1, for state member banks; FDIC *Manual of Examination Policies,* section 11.1, for insured state nonmember banks; and OTS *Thrift Activities Handbook,* section 211, for savings associations.

Pre-purchase Analysis

The objective of the pre-purchase analysis is to help ensure that the institution understands the risks, rewards, and unique characteristics of BOLI. The nature and extent of this analysis should be commensurate with the size and complexity of the potential BOLI purchases and should also take into account existing BOLI holdings. A mark of a well-managed institution is the maintenance of adequate records concerning its pre-purchase analyses, usually including documentation of the purpose and amount of insurance needed.

An effective pre-purchase analysis involves the following management actions:

Step 1—Identify the need for insurance and determine the economic benefits and appropriate insurance type. An institution should determine the need for insurance by identifying the specific risk of loss to which it is exposed or the specific costs to be recovered. It is not appropriate to purchase life insurance to recover a loss that the institution has already incurred. An institution's purchase of insurance to indemnify it against a specific risk of loss does not relieve it from other responsibilities related to managing that risk. The type of BOLI product, e.g., general[5] or separate account, and its features should be appropriate to meet the identified needs of the institution. The appendix [appendix A] contains a description of insurance types and design features.

An institution should analyze the cost and benefits of planned BOLI purchases. The analysis should include the anticipated performance of the BOLI policy and an assessment of how the purchase will accomplish the institution's objectives. Before purchasing BOLI, an institution should analyze projected policy values (CSV and death benefits) using multiple illustrations of these projections provided by the carrier, some of which incorporate the institution's own assumptions. An institution should consider using a range of interest-crediting rates and mortality-cost assumptions. In some cases, the net yield (after mortality costs) could be negative, particularly for separate-account products. The potential for unfavorable net yields underscores the importance of carefully evaluating BOLI costs and benefits across multiple scenarios, both currently and into the future.

Step 2—Quantify the amount of insurance appropriate for the institution's objectives. An institution should estimate the size of the employee benefit obligation or the risk of loss to be covered and ensure that the amount of BOLI purchased is not excessive in relation to this estimate and the associated product risks. When using BOLI to recover the cost of providing employee benefits, the estimated present value of the expected future cash flows from BOLI, less the costs of insurance, should not exceed the estimated present value of the expected after-tax employee benefit costs. In situations where an institution purchases BOLI on a group of eligible employees, it may estimate the size of the obligation or the risk of loss for the group on an aggregate basis and compare that to the aggregate amount of insurance to be purchased. This estimate should be based on reasonable financial and actuarial assumptions. State insurable interest laws may further restrict or limit the amount of insurance that may be purchased on a group of employees. Management must be able to support, with objective evidence, the reasonableness of all of the assumptions used in determining the appropriate amount of insurance coverage needed by the institution, including the rationale for its discount rates and cost projections.

Step 3—Assess the vendor's qualifications. When making a decision about vendors, an institution should consider its own knowledge of insurance risks, the vendor's qualifications, and the amount of resources the institution is willing to spend to administer and service the BOLI. Depending on the role of the vendor, the vendor's services can be extensive and may be critical to successful implementation and operation of a BOLI plan, particularly for the more complex separate-account products.

While it is possible to purchase insurance directly from insurance carriers, the vast majority of insurance purchases are made through vendors—either brokers, consultants, or agents. A vendor may design, negotiate, and administer the BOLI policy. An institution should ensure that it understands the product it is purchasing and that it selects a product that best meets its needs. Management, not just the vendor, must demonstrate a familiarity with the technical

5. A general account is a design feature that is generally available to purchasers of whole or universal life insurance whereby the general assets of the insurance company support the policyholder's CSV.

details of the institution's insurance assets, and be able to explain the reasons for and the risks associated with the product design features they have selected.

An institution that uses a vendor should make appropriate inquiries to satisfy itself about the vendor's ability to honor its long-term commitments, particularly when the vendor is expected to be associated with the institution's insurance program over an extended period of time. The institution should evaluate the adequacy of the vendor's services and its reputation, experience, financial soundness, and commitment to the BOLI product. Vendors typically earn a large portion of their commissions upon the sale of the product, yet they often retain long-term servicing responsibilities for their clients. The vendor's commitment to investing in the operational infrastructure necessary to support BOLI is a key consideration in vendor selection.

An institution should be aware that the vendor's financial benefit from the sale of insurance may provide the vendor with an incentive to emphasize the benefits of a BOLI purchase to the institution without a commensurate explanation of the associated risks. Therefore, reliance solely upon pre-packaged, vendor-supplied compliance information does *not* demonstrate prudence with respect to the purchase of insurance. An institution should not delegate its selection of product design features to its vendors. An institution that is unable to demonstrate a thorough understanding of BOLI products it has purchased and the associated risks may be subject to supervisory action.

Step 4—Review the characteristics of the available insurance products. There are a few basic types of life insurance products in the marketplace. These products, however, can be combined and modified in many different ways. The resulting final product can be quite complex. Furthermore, certain permanent insurance products have been designed specifically for banks. These products differ from other forms of corporate-owned life insurance (COLI) policies in that the policies designed for banks are generally structured without surrender or front-end sales charges in order to avoid having to report these charges as expenses when initially recording the carrying value. However, BOLI products may have lower net yields than COLI products due to the absence of these charges. An institution should review the characteristics of the various insurance products available, understand the products it is considering purchasing, and select those with the characteristics that best match the institution's objectives, needs, and risk tolerance.

Design features of permanent insurance policies determine (1) whether the policy is a general account, separate account, or hybrid product;[6] (2) whether the insurance contract is a modified endowment contract (MEC) that carries certain tax penalties if surrendered; and (3) the method used to credit earnings to the policy. Some implications of these design features are discussed in more detail in the "Risk Management of BOLI" section of this interagency statement.

When purchasing insurance on a key person or a borrower, management should consider whether the institution's need for the insurance might end before the insured person dies. An institution generally may not hold BOLI on a key person or a borrower once the key person leaves the institution or the borrower has either repaid the loan, or the loan has been charged off. Therefore, the maturity of the term or declining term insurance should be structured to match the expected tenure of the key person or the maturity of the loan, respectively. Permanent insurance generally is not an appropriate form of life insurance under these circumstances.

Step 5—Select the carrier. To achieve the tax benefits of insurance, institutions must hold BOLI policies until the death of the insured. Therefore, carrier selection is one of the most critical decisions in a BOLI purchase and one that can have long-term consequences. While a broker or consultant may assist the institution in evaluating carrier options, the institution alone retains the responsibility for carrier selection. Before purchasing life insurance, an institution should perform a credit analysis on the selected carrier(s) in a manner consistent with safe and sound banking practices for commercial lending. A more complete discussion of the credit-analysis standards is included in the "Credit Risk" section of this interagency statement.

Management should review the product design, pricing, and administrative services of proposed carriers and compare them with the institution's needs. Management should also review the carrier's commitment to the BOLI product, as well as its credit ratings, general reputation, experi-

6. A hybrid product combines features of both general- and separate-account products.

ence in the marketplace, and past performance. Carriers not committed to general-account BOLI products may have an incentive to lower the interest-crediting rate on BOLI over time, reducing the favorable economics of the product. The interest-crediting rate refers to the gross yield on the investment in the insurance policy, that is, the rate at which the cash value increases before considering any deductions for mortality cost, load charges, or other costs that are periodically charged against the policy's cash value. Insurance companies frequently disclose both a current interest-crediting rate and a guaranteed minimum interest-crediting rate. Institutions should be aware that the guaranteed minimum interest-crediting rate may be periodically reset in accordance with the terms of the insurance contract. As a result, the potential exists for a decline in the interest-crediting rate.

While institutions can exercise what is known as a 1035 exchange[7] option to change carriers, there are some practical constraints to using this option. First, the institution must have an insurable interest in each individual to be insured under the new carrier's policy. In a 1035 exchange, former employees of the institution may not be eligible for coverage under the new policy because state insurable interest laws may prohibit their eligibility. Second, the original carrier may impose an exchange fee specifically applicable to such 1035 exchanges.

Step 6—Determine the reasonableness of compensation provided to the insured employee if the insurance results in additional compensation. Insurance arrangements that are funded by the institution and that permit the insured officer, director, or employee to designate a beneficiary are a common way to provide additional compensation or other benefits to the insured. Split-dollar life insurance arrangements are often used for this purpose. Before an institution enters into a split-dollar arrangement or otherwise purchases insurance for the benefit of an officer, director, or employee, the institution should identify and quantify its compensation objective and ensure that the arrangement is consistent with that objective. The compensation provided by the split-dollar or other insurance arrangement should be combined with all other compensation provided to the insured to ensure that the insured's total compensation is not excessive. Excessive compensation is considered an unsafe and unsound banking practice. Guidelines for determining excessive compensation can be found in the Interagency Guidelines Establishing Standards for Safety and Soundness.[8]

Because shareholders and their family members who are not officers, directors, or employees of an institution do not provide goods or services to the institution, they should not receive compensation from the institution. This includes compensation in the form of split-dollar life insurance arrangements.

Prior to an institution's purchase of a life insurance policy to be used in a split-dollar life insurance arrangement, the institution and the insured should enter into a written agreement. Written agreements usually describe the rights of the institution, the insured individual, and any other parties (such as trusts or beneficiaries) to the policy's CSV and death benefits. It is important for an institution to be aware that ownership of the policy by the employee, a third party, or a trust (non-institution owner) may not adequately protect the institution's interest in the policy because the institution ordinarily will not have the sole right to borrow against the CSV or to liquidate the policy in the event that funds are needed to provide liquidity to the institution. Moreover, if a non-institution owner borrows heavily against the CSV, an institution's ability to recover its premium payments upon the death of the insured may be impaired.

At a minimum, an institution's economic interest in the policy should be equal to the premiums paid plus a reasonable rate of return, defined as a rate of return that is comparable to returns on investments of similar maturity and credit risk.

Split-dollar life insurance has complex tax and legal consequences. An institution considering entering into a split-dollar life insurance arrangement should consult qualified tax, legal, and insurance advisers.

Step 7—Analyze the associated risks and the ability to monitor and respond to those risks. An institution's pre-purchase analysis should include a thorough evaluation of all significant risks, as

7. A 1035 exchange is a tax-free replacement of an insurance policy for another insurance contract covering the same person in accordance with section 1035 of the Internal Revenue Code.

8. For national banks, appendix A to 12 CFR 30; for state member banks, appendix D-1 to 12 CFR 208; for insured state nonmember banks, appendix A to 12 CFR 364; for savings associations, appendix A to 12 CFR 570.

well as management's ability to identify, measure, monitor, and control those risks. An explanation of key risks (liquidity, transaction/operational, reputation, credit, interest rate, compliance/legal, and price) is included in the "Risk Management of BOLI" section of this interagency statement.

Step 8—Evaluate the alternatives. Regardless of the purpose of BOLI, a comprehensive pre-purchase analysis will include an analysis of available alternatives. Prior to acquiring BOLI, an institution should thoroughly analyze the risks and benefits, compared to alternative methods for recovering costs associated with the loss of key persons, providing pre- and post-retirement employee benefits, or providing additional employee compensation, as appropriate.

Step 9—Document the decision. A well-managed institution maintains adequate documentation supporting its comprehensive pre-purchase analysis, including an analysis of both the types and design of products purchased and the overall level of BOLI holdings.

Risk Management of BOLI

Risk assessment and risk management are vital components of an effective BOLI program. In addition to conducting a risk assessment as part of a thorough pre-purchase analysis, monitoring BOLI risks on an ongoing basis is important, especially for an institution whose aggregate BOLI holdings represent a capital concentration. Management of an institution should review the performance of the institution's insurance assets with its board of directors at least annually. More-frequent reviews are appropriate if there are significant anticipated changes to the BOLI program such as additional purchases, a decline in the financial condition of the insurance carrier(s), anticipated policy surrenders, or changes in tax laws or interpretations that could have an impact on the performance of BOLI. This risk-management review should include, but not necessarily be limited to:

- *Comprehensive assessment of the specific risks discussed in this section.*[9]
- *Identification of which employees are, or will be, insured (e.g., vice presidents and above, employees of a certain grade level).* For example, an institution that acquires another institution that owns BOLI may acquire insurance on individuals that it would not insure under its own standards. While the acquiring institution need not correct such exceptions, it is important to know that such exceptions exist.
- *Assessment of death benefit amounts relative to employee salaries.* Such information helps management to assess the reputation and insurable interest risks associated with disproportionately large death benefits.
- *Calculation of the percentage of insured persons still employed by the institution.* Larger institutions often find that their policies insure more former employees than current employees. This information can help the institution assess reputation risk.
- *Evaluation of the material changes to BOLI risk-management policies.*
- *Assessment of the effects of policy exchanges.* Exchanges typically are costly and it is a sound practice to review the costs and benefits of such actions.
- *Analysis of mortality performance and impact on income.* Material gains from death benefits can create reputation risks.
- *Evaluation of material findings from internal and external audits and independent risk-management reviews.*
- *Identification of the reason for, and tax implications of, any policy surrenders.* In some cases, institutions have surrendered BOLI policies and incurred tax liabilities and penalties. Formal assessment of the costs and benefits of a surrender is a useful component of sound corporate governance.
- *Peer analysis of BOLI holdings.* To address reputation risk, an institution should compare its BOLI holdings relative to capital to the holdings of its peers to assess whether it is an outlier.

Liquidity Risk

Liquidity risk is the risk to earnings and capital arising from an institution's inability to meet its obligations when they come due without incur-

9. All of the risks discussed in this section are applicable to permanent insurance. In contrast, because temporary insurance does not have a savings component or a CSV, it does not expose an institution to liquidity, interest-rate, or price risk. These risks need not be evaluated in the comprehensive assessment of the risks of temporary insurance.

ring unacceptable losses. Before purchasing permanent insurance, management should recognize the illiquid nature of the product and ensure that the institution has the long-term financial flexibility to hold the asset in accordance with its expected use. The inability to hold the life insurance until the death(s) of the insured(s) when the death benefits will be collected may compromise the success of the BOLI plan. An institution generally does not receive any cash flow from the insurance until the death benefit is paid. Depending upon the age of the insured population, it is possible that an institution that insures a small number of employees may not recognize any cash flow from the insurance for many years. The illiquid nature of insurance assets, combined with the difficulty of projecting liquidity needs far into the future, is a major reason an institution should keep its BOLI holdings below the agencies' concentration guidelines. Examiners will consider an institution's BOLI holdings when assessing liquidity and assigning the liquidity component rating.

The purchase of BOLI may negatively affect an institution's liquidity position, both because BOLI is one of the least liquid assets on an institution's balance sheet, and because institutions normally fund BOLI purchases through the sale of liquid assets (e.g., marketable securities). To access the CSV of BOLI, the institution must either surrender or borrow against the policy. In accordance with the policy contract and federal tax laws, the surrender of a policy may subject an institution to surrender charges, tax liabilities for previously untaxed increases in the CSV, and tax penalties. Borrowing against the CSV is disadvantageous in most cases due to limitations on the ability to deduct interest on the borrowing and other possible adverse tax consequences.

A BOLI product qualifying as a modified endowment contract (MEC) for tax purposes has particular liquidity disadvantages. If an institution surrenders a MEC, it will incur a tax liability on the increase in the policy's CSV from earnings on the policy since its inception and may incur an additional tax penalty for early surrender.

In order to avoid such additional tax penalties, an institution may opt to purchase a non-MEC contract. A non-MEC contract permits the policy owner to surrender the policy without incurring the additional tax penalty that, under certain circumstances, applies to MECs. Moreover, depending on the terms of the insurance contract, an institution generally may withdraw up to the basis (that is, the original amount invested) without creating a taxable event. However, a non-MEC policy increases in complexity if it is in the form of a separate account covered by a stable value protection (SVP) contract. An SVP contract protects the policy owner from declines in the value of the assets in the separate account arising from changes in interest rates, thereby mitigating price risk and earnings volatility. An SVP contract is most often used in connection with fixed-income investments. Institutions should recognize that SVP providers often place restrictions on the amount that may be withdrawn from the separate account, thereby reducing the liquidity of the BOLI asset. An institution considering the purchase of a non-MEC for its potential liquidity advantages compared to a MEC also should be aware of contractual provisions, such as 1035 exchange fees and "crawl-out" restrictions,[10] which may limit such advantages.

Transaction/Operational Risk

As it applies to BOLI, transaction/operational risk is the risk to earnings and capital arising from problems caused by the institution's failure to fully understand or to properly implement a transaction. Transaction/operational risk arises due to the variety and complexity of life insurance products, as well as tax and accounting treatments. To help mitigate this risk, management should have a thorough understanding of how the insurance product works and the variables that dictate the product's performance. The variables most likely to affect product performance are the policy's interest-crediting rate, mortality cost, and other expense charges.

Transaction/operational risk is also a function of the type and design features of a life insurance contract. With a general-account product, there are only two parties to the contract: the policy owner and the insurance carrier. With a separate-account product, the insurance carrier has a separate contract with an investment manager. There could also be an SVP provider with whom the carrier has a separate contract.

Transaction/operational risk may also arise as a result of the variety of negotiable features associated with a separate-account product.

10. A crawl-out restriction limits the amount of CSV eligible for a 1035 exchange or surrender over a period of time.

These include the investment options; the terms, conditions, and cost of SVP; and mortality options. Deferred acquisition costs (DAC) represent the insurance carrier's up-front costs associated with issuing an insurance policy, including taxes and commissions and fees paid to agents for selling the policy. The carrier charges the policyholder for these costs and capitalizes the DAC, including the prepayment of taxes in accordance with federal tax law. As the carrier recovers the DAC in accordance with applicable tax law, it credits the amount to the separate-account policyholder. Once it has been credited to the institution, the DAC is essentially a receivable from the carrier and, therefore, represents a general-account credit exposure.

Separate-account policies have additional transaction risks that can result from accounting requirements. Several institutions have had to restate their earnings because of contractual provisions in their policies that were ambiguous with respect to the amount of the CSV available upon surrender of the policy. Because BOLI must be carried at the amount that could be realized under the insurance contract as of the balance-sheet date, if any contractual provision related to costs, charges, or reserves creates uncertainty regarding the realization of a policy's full CSV, the agencies will require an institution to record the BOLI net of those amounts. As part of an effective pre-purchase analysis, an institution should thoroughly review and understand how the accounting rules will apply to the BOLI policy it is considering purchasing.

Tax and Insurable Interest Implications

Before the purchase of BOLI and periodically thereafter, management should also explicitly consider the financial impact (e.g., tax provisions and penalties) of surrendering a policy. Recent adverse press coverage of corporate-owned life insurance (COLI) should serve as a reminder to institutions that the current tax law framework, as it applies to BOLI, is always subject to legislative changes. A tax change that makes future BOLI cash flows subject to income tax, while perhaps deemed unlikely by many institutions, would have a negative impact on the economics of the BOLI holdings. An institution should recognize that earnings from BOLI could make it subject to the alternative minimum tax.

Institutions should also recognize that their actions, subsequent to purchase, could jeopardize the tax-advantaged status of their insurance holdings. The risk that a life insurance policy could be characterized by the Internal Revenue Service (IRS) as an actively managed investment is particularly relevant to separate-account policies. Many larger institutions prefer separate-account products because of perceived lower credit risk and greater transparency (that is, explicit disclosure of costs). Assets held by the insurance company on behalf of the policy owners in the separate account are intended to be beyond the reach of the insurance company's general creditors in the event of insolvency; however, the protected status of separate-account assets is generally untested in the courts. While the separate-account structure helps to mitigate an institution's credit exposure to the insurance carrier, the institution can have no "control" over investment decisions (e.g., timing of investments or credit selection) in the underlying account. Generally, allocating separate-account holdings across various divisions of an insurance company's portfolio does not raise concerns about "control," but other actions that a policy owner takes may be construed as investment control and could jeopardize the tax-advantaged status.

To benefit from the favorable tax treatment of insurance, a BOLI policy must be a valid insurance contract under applicable state law and must qualify under applicable federal law. Institutions must have an insurable interest in the covered employee, as set forth in applicable state laws. Furthermore, the favorable tax-equivalent yields of BOLI result only when an institution generates taxable income. Institutions that have no federal income tax liability receive only the nominal interest-crediting rate as a yield. In such an environment, BOLI loses much of its yield advantage relative to other investment alternatives.

Some institutions seem to have drawn comfort from assurances from insurance carriers that the carrier would waive lack of insurable interest as a defense against paying a claim. While the carrier may indeed make a payment, such payment may not necessarily go to the institution. Such assurances may not be sufficient to satisfy the IRS requirements for a valid insurance contract, nor do they eliminate potential claims from the estate of the insured that might seek to claim insurance proceeds on the basis that the institution lacked an insurable interest.

For example, some institutions have established out-of-state trusts to hold their BOLI assets. While such trusts may have legitimate uses, such as to gain access to an insurance carrier's product, in some cases the purpose is to avoid unfavorable insurable interest laws in the institution's home state and to domicile the policy in a state with more lenient requirements. In some cases, institutions have not made employees aware that they have taken out insurance on their lives.

A recent Fifth Circuit Court of Appeals ruling demonstrates the potential danger of this approach. A Texas employer used a Georgia trust to hold life insurance policies on its employees in Texas, and the trust agreement provided that the insurable interest law of Georgia should apply. In a lawsuit brought by the estate of a deceased employee, the court ignored this provision because the insured employee was not a party to the trust agreement. It then found that the insurable interest law of Texas applied and under that state's law, the employer did not have an insurable interest in the employee. The result was that the employer was not entitled to the insurance death benefits.[11] The outcome in this case suggests that institutions that have used, or are considering using, an out-of-state trust to take advantage of more-favorable insurable interest laws in another state should assess whether they could be vulnerable to a similar legal challenge.

Institutions should have appropriate legal review to help ensure compliance with applicable tax laws and state insurable interest requirements. Institutions that insure employees for excessive amounts may be engaging in impermissible speculation or unsafe and unsound banking practices. The agencies may require institutions to surrender such policies.

Reputation Risk

Reputation risk is the risk to earnings and capital arising from negative publicity regarding an institution's business practices. While this risk arises from virtually all bank products and services, reputation risk is particularly prevalent in BOLI because of the potential perception issues associated with an institution's owning or benefiting from life insurance on employees.

A well-managed institution will take steps to reduce the reputation risk that may arise as a result of its BOLI purchases, including maintaining appropriate documentation evidencing informed consent by the employee, prior to purchasing insurance. Some institutions assert that they make employees aware via employee handbooks, manuals, or newsletters of the possibility that the institution may acquire life insurance on them. Although such disclosure may satisfy state insurance requirements, any approach that does not require formal employee consent may significantly increase an institution's reputation risk.

Some institutions have begun to purchase separate-account, non-MEC product designs in order to address the liquidity concerns with MEC policies. One consequence of this product design choice, however, is that it has become increasingly common for institutions to insure a very large segment of their employee base, including non-officers. Because non-MEC designs have a higher ratio of death benefit to premium dollar invested, some institutions have, therefore, taken out very high death benefit policies on employees, including lower-level employees, further adding to reputation risk and highlighting the importance of obtaining explicit consent.

Credit Risk

Credit risk is the potential impact on earnings and capital arising from an obligor's failure to meet the terms of any contract with the institution or otherwise perform as agreed. All life insurance policyholders are exposed to credit risk. The credit quality of the insurance company and duration of the contract are key variables. With insurance, credit risk arises from the insurance carrier's contractual obligation to pay death benefits upon the death of the insured, and if applicable, from the carrier's obligation to pay the CSV (less any applicable surrender charges) upon the surrender of the policy.

Most BOLI products have very long-term (30- to 40-year) expected time frames for full collection of cash proceeds, i.e., the death benefit. For general-account policies, the CSV is an unsecured, long-term, and nonamortizing obligation of the insurance carrier. Institutions record and carry this claim against the insurance company as an asset.

11. Mayo v. Hartford Life Insurance Company, 354 F.3d 400 (5th Cir. 2004).

Before purchasing BOLI, an institution should conduct an independent financial analysis of the insurance company and continue to monitor its condition on an ongoing basis. The institution's credit-risk-management function should participate in the review and approval of insurance carriers. As with lending, the depth and frequency of credit analysis (both initially and on an ongoing basis) should be a function of the relative size and complexity of the transaction and the size of outstanding exposures. Among other things, an institution should consider its legal lending limit, concentration guidelines (generally defined as the aggregate of direct, indirect, and contingent obligations and exposures that exceed 25 percent of the institution's capital), and any applicable state restrictions on BOLI holdings when assessing its broader credit-risk exposure to insurance carriers. To measure credit exposures comprehensively, an institution should aggregate its exposures to individual insurance carriers, and the insurance industry as a whole, attributable to both BOLI policies and other credit relationships (e.g., loans and derivatives exposures).

There are product design features of a BOLI policy that can reduce credit risk. As noted earlier, an institution can purchase separate-account products, where the institution assumes the credit risk of the assets held in the separate account, rather than the direct credit risk of the carrier as would be the case in a general-account policy. With separate-account policies, the insurance carrier owns the assets, but maintains the assets beyond the reach of general creditors in the event of the insurer's insolvency. However, even with a separate-account policy, the policy owner incurs some general-account credit-risk exposure to the insurance carrier associated with the carrier's mortality and DAC reserves. Amounts equal to the mortality and DAC reserves are owed to the policyholder and represent general-account obligations of the insurance carrier. In addition, the difference, if any, between the CSV and the minimum guaranteed death benefit would be paid out of the insurance carrier's general account.

A separate-account policy may have a stable value protection (SVP) contract issued by the insurance carrier or by a third party that is intended to protect the policyholder from most declines in fair value of separate-account assets. In general, the provider of an SVP contract agrees to pay any shortfall between the fair value of the separate-account assets when the policy owner surrenders the policy and the cost basis of the separate account to the policy owner. Under most arrangements, the insurance carrier is not responsible for making a payment under the SVP contract if a third-party protection provider fails to make a required payment to it. The SVP contract thus represents an additional source of credit risk for a separate-account product. The policyholder's exposure under an SVP contract is to both the protection provider, which must make any required payment to the insurance carrier, and the carrier, which must remit the payment received from the protection provider to the institution. Because of this exposure, an institution should also evaluate the repayment capacity of the SVP provider.

State insurance regulation governing reserve requirements for insurance carriers, state guaranty funds, and reinsurance arrangements help to reduce direct credit risks from general-account exposures. Further, an institution can use a 1035 exchange to exit a deteriorating credit exposure, although most policies impose fees for the exchange. While credit risk for existing general- and separate-account policies may be low currently, the extremely long-term nature of a BOLI policy underscores the fact that credit risk remains an important risk associated with life insurance products. Strong current credit ratings offer no guarantee of strong credit ratings 20, 30, or 40 years into the future.

Interest-Rate Risk

Interest-rate risk is the risk to earnings and capital arising from movements in interest rates. Due to the interest-rate risk inherent in general-account products, it is particularly important that management fully understand how these products expose the policyholder to interest-rate risk before purchasing the policy. The interest-rate risk associated with these products is primarily a function of the maturities of the assets in the carrier's investment portfolio, which often range from four to eight years. When purchasing a general-account policy, an institution chooses one of a number of interest-crediting options (that is, the method by which the carrier will increase the policy's CSV). Using the "portfolio" crediting rate, the institution will earn a return based upon the existing yield of the carrier's portfolio each year. Using the "new money" crediting rate, the institution earns a

return based upon yields available in the market at the time it purchases the policy.

Separate-account products may also expose the institution to interest-rate risk, depending on the types of assets held in the separate account. For example, if the separate-account assets consist solely of U.S. Treasury securities, the institution is exposed to interest-rate risk in the same way as holding U.S. Treasury securities directly in its investment portfolio. However, because the institution cannot control the separate-account assets, it is more difficult for the institution to control this risk. Accordingly, before purchasing a separate-account product, an institution's management should thoroughly review and understand the instruments governing the investment policy and management of the separate account. Management should understand the risk inherent within the separate account and ensure that the risk is appropriate for the institution. The institution also should establish monitoring and reporting systems that will enable management to monitor and respond to interest-rate fluctuations and their effect on separate-account assets.

Compliance/Legal Risk

Compliance/legal risk is the risk to earnings and capital arising from violations of, or nonconformance with, laws, rulings, regulations, prescribed practices, or ethical standards. Failure to comply with applicable laws, rulings, regulations, and prescribed practices could compromise the success of a BOLI program and result in fines or penalties imposed by regulatory authorities or loss of tax benefits. Among the legal and regulatory considerations that an institution should evaluate are compliance with state insurable interest laws, the Employee Retirement Income Security Act of 1974 (ERISA), Federal Reserve Regulations O and W (12 CFR 215 and 223, respectively), the Interagency Guidelines Establishing Standards for Safety and Soundness, the requirements set forth under the "Legal Authority" section of this document, and federal tax regulations applicable to BOLI.

Tax benefits are critical to the success of most BOLI plans. Accordingly, an institution owning separate-account BOLI must implement internal policies and procedures to ensure that it does not take any action that might be interpreted as exercising "control" over separate-account assets. This is especially important for privately placed policies in which the institution is the only policyholder associated with the separate-account assets.

When purchasing BOLI, institutions should be aware that the splitting of commissions between a vendor and the institution's own subsidiary or affiliate insurance agency presents compliance risk. The laws of most states prohibit the payment of inducements or rebates to a person as an incentive for that person to purchase insurance. These laws may also apply to the person receiving the payment. When an insurance vendor splits its commission with an institution's insurance agency that was not otherwise involved in the transaction, such a payment may constitute a prohibited inducement or rebate. Accordingly, an institution should assure itself that this practice is permissible under applicable state law and in compliance with Federal Reserve Regulation W before participating in any such arrangement. Moreover, payments to an affiliate that did not perform services for the institution could also raise other regulatory and supervisory issues.

Due to the significance of the compliance risk, institutions should seek the advice of counsel on these legal and regulatory issues.

Price Risk

Price risk is the risk to earnings and capital arising from changes in the value of portfolios of financial instruments. Accounting rules permit owners of insurance contracts to account for general-account products using an approach that is essentially based on cost plus accrued earnings. However, for separate-account products without SVP, the accounting would largely be based on the fair value of the assets held in the account because this value is the amount that could be realized from the separate account if the policy is surrendered. (See "Accounting Considerations" above.) Typically, the policyholder of separate-account products assumes all price risk associated with the investments within the separate account. Usually, the insurance carrier will provide neither a minimum CSV nor a guaranteed interest-crediting rate for separate-account products. Absent an SVP contract, the amount of price risk generally depends upon the type of assets held in the separate account.

Because the institution does not control the separate-account assets, it is more difficult for it to control the price risk of these assets than if

they were directly owned. To address income-statement volatility, an institution may purchase an SVP contract for its separate-account policy. The SVP contract is designed to ensure that the amount that an institution could realize from its separate-account policy, in most circumstances, remains at or above the cost basis of the separate account to the policyholder. Institutions should understand, however, that SVP contracts protect against declines in value attributable to changes in interest rates; they do not cover default risk. Moreover, one purpose of the SVP contract is to reduce volatility in an institution's reported earnings. To realize any economic benefit of the SVP contract, an institution would have to surrender the policy. Since policy surrender is nearly always an uneconomic decision, the SVP contract provides, in a practical sense, accounting benefits only.

Before purchasing a separate-account life insurance product, management should thoroughly review and understand the instruments governing the investment policy and management of the separate account. Management should understand the risk inherent in the separate account and ensure that the risk is appropriate. If the institution does not purchase SVP, management should establish monitoring and reporting systems that will enable it to recognize and respond to price fluctuations in the fair value of separate-account assets.

Under limited circumstances it is legally permissible for an institution to purchase an equity-linked variable life insurance policy if the policy is an effective economic hedge against the institution's equity-linked obligations under employee benefit plans.[12] An effective economic hedge exists when changes in the economic value of the liability or other risk exposure being hedged are matched by counterbalancing changes in the value of the hedging instrument. Such a relationship would exist where the obligation under an institution's deferred compensation plan is based upon the value of a stock market index and the separate account contains a stock mutual fund that mirrors the performance of that index. Institutions need to be aware that this economic hedge may not qualify as a hedge for accounting purposes. Thus, the use of equity-linked variable life insurance policies to economically hedge equity-linked obligations may not have a neutral effect on an institution's reported earnings.

Unlike separate-account holdings of debt securities, SVP contracts on separate-account equity holdings are not common. The economic hedging criteria for equity-linked insurance products lessen the effect of price risk because changes in the amount of the institution's equity-linked liability are required to offset changes in the value of the separate-account assets. If the insurance cannot be characterized as an effective economic hedge, the presence of equity securities in a separate account is impermissible, and the agencies will require institutions to reallocate the assets unless retention of the policy is permitted under federal law.[13]

In addition to the general considerations discussed previously, which are applicable to any separate-account product, an institution should perform further analysis when purchasing a separate-account product involving equity securities. At a minimum, the institution should:

1. Compare the equity-linked liability being hedged (e.g., deferred compensation) and the equity securities in the separate account. Such an analysis considers the correlation between the liability and the equity securities, expected returns for the securities (including standard deviation of returns), and current and projected asset and liability balances.
2. Determine a target range for the hedge effectiveness ratio (e.g., 95 to 105 percent) and establish a method for measuring hedge effectiveness on an ongoing basis. The institution should establish a process for altering the program if hedge effectiveness drops below acceptable levels. Consideration should be given to the potential costs of program changes.
3. Establish a process for analyzing and reporting to management and the board the effect of the hedge on the institution's earnings and capital ratios. The analysis usually considers results both with and without the hedging transaction.

12. Insured state banks and state savings associations may make such purchases only if permitted to do so under applicable state law.

13. Insured state banks and state savings associations may request the FDIC's consent to retain the policies, but consent will not be granted if it is determined that retaining the policies presents a significant risk to the appropriate insurance fund.

Risk-Based Capital Treatment

If an institution owns a general-account insurance product, it should apply a 100 percent risk weight to its claim on the insurance company for risk-based capital purposes. A BOLI investment in a separate-account insurance product, however, may expose the institution to the market and credit risks associated with the pools of assets in the separate account. The assets in a pool may have different risk weights, similar to the assets held in a mutual fund in which an institution has invested. For risk-based capital purposes, if an institution can demonstrate that the BOLI separate-account policy meets the requirements below, it may choose to "look through" to the underlying assets to determine the risk weight.

Criteria for a Look-Through Approach

To qualify for the "look-through" approach, separate-account BOLI assets must be protected from the insurance company's general creditors in the event of the insurer's insolvency. An institution should document its assessment, based upon applicable state insurance laws and other relevant factors, that the separate-account assets would be protected from the carrier's general creditors. If the institution does not have sufficient information to determine that a BOLI separate-account policy qualifies for the look-through approach, the institution must apply the standard risk weight of 100 percent to this asset.

In addition, when an institution has a separate-account policy, the portion of the carrying value of the institution's insurance asset that represents general-account claims on the insurer, such as deferred acquisition costs (DAC) and mortality reserves that are realizable as of the balance-sheet date, and any portion of the carrying value attributable to an SVP contract, are not eligible for the look-through approach. These amounts should be risk-weighted at the 100 percent risk weight applicable to claims on the insurer or the SVP provider, as appropriate.

Look-Through Approaches

When risk-weighting a qualifying separate-account policy, an institution may apply the highest risk weight for an asset permitted in the separate account, as stated in the investment agreement, to the entire carrying value of the separate-account policy, except for any portions of the carrying value that are general-account claims or are attributable to SVP. In no case, however, may the risk weight for the carrying value of the policy (excluding any general-account and SVP portions) be less than 20 percent.

Alternatively, an institution may use a pro rata approach to risk-weighting the carrying value of a qualifying separate-account policy (excluding any general-account and SVP portions). The pro rata approach is based on the investment limits stated in the investment agreement for each class of assets that can be held in the separate account, with the constraint that the weighted average risk weight may not be less than 20 percent. If the sum of the permitted investments across market sectors in the investment agreement is greater than 100 percent, the institution must use the highest risk weight for the maximum amount permitted in that asset class, and then proceed to the next-highest risk weight until the permitted amounts equal 100 percent.

For example, if a separate-account investment agreement permits a maximum allocation of 60 percent for corporate bonds, 40 percent for U.S. government–sponsored enterprise debt securities, and 60 percent for U.S. Treasury securities, then the institution must risk-weight 60 percent of the carrying value of the separate-account investment (excluding any portion attributable to SVP) at the 100 percent risk weight applicable to corporate bonds and the remaining 40 percent at the 20 percent risk weight for U.S. government–sponsored enterprise debt securities. Because the sum of the permitted allocation for corporate bonds and government-sponsored enterprise debt securities totals 100 percent, the institution cannot use the zero percent risk weight for U.S. Treasury securities. However, if the permitted allocation for U.S. government–sponsored enterprise debt securities was 30 percent rather than 40 percent, the institution could risk-weight the remaining 10 percent of the carrying value of its investment at the zero percent risk weight for U.S. Treasuries.

Regardless of the look-through approach an institution employs, the weighted average risk weight for the separate-account policy (excluding any general-account and SVP portions) may not be less than 20 percent, even if all the assets in the separate account would otherwise qualify

for a zero percent risk weight. Furthermore, the portion of the carrying value of the separate-account policy that represents general-account claims on the insurer, such as realizable DAC and mortality reserves, and any portion of the carrying value attributable to an SVP contract, should be risk-weighted at the risk weight applicable to the insurer or the SVP provider, as appropriate.

The following example demonstrates the appropriate risk-weight calculations for the pro rata approach, incorporating the components of a BOLI separate-account policy that includes general-account claims on the insurer as well as the investment allocations permitted for different asset classes in the separate-account investment agreement.

Example. The separate-account investment agreement requires the account to hold a minimum of 10 percent in U.S. Treasury obligations. It also imposes a maximum allocation of 50 percent in mortgage-backed securities issued by U.S. government–sponsored enterprises, and a maximum allocation of 50 percent in corporate bonds. Assume that the portion of the carrying value of the separate-account policy attributable to realizable DAC and mortality reserves equals $10 and that the portion attributable to the SVP totals $10.

Carrying value of separate-account policy	$100.00
Less: Portion attributable to DAC and mortality reserves	10.00
Portion attributable to SVP	10.00
Net carrying value of separate-account policy available for pro rata	$ 80.00
Risk-weight calculation:	
U.S. Treasury @ 10% x $80 = $8 x 0% RW	0.00
Corporate bonds @ 50% x $80 = $40 x 100% RW	$ 40.00
GSE MBS @ 40% x $80 = $32 x 20% RW	6.40
Separate-account risk-weighted assets subject to pro rata	$ 46.40
Add back: DAC and mortality reserves = $10 x 100% RW	$ 10.00
Add back: SVP = $10 x 100% RW	10.00
General-account and SVP risk-weighted assets	$ 20.00
Total BOLI-related risk-weighted assets	$ 66.40

Summary

The purchase of BOLI can be an effective way for institutions to manage exposures arising from commitments to provide employee compensation and pre- and post-retirement benefits. Consistent with safe and sound banking practices, institutions must understand the risks associated with this product and implement a risk-management process that provides for the identification and control of such risks. A sound pre-purchase analysis, meaningful ongoing monitoring program, reliable accounting process, and accurate assessment of risk-based capital requirements are all components of the type of risk-management process the agencies expect institutions to employ.

Where an institution has acquired BOLI in an amount that approaches or exceeds agency concentration levels, examiners will more closely scrutinize the components of the risk-management process and the institution's associated documentation. Where BOLI has been purchased in an impermissible manner, ineffective controls over BOLI risks exist, or a BOLI exposure poses a safety-and-soundness concern, the appropriate agency may take supervisory action, including requiring the institution to divest affected policies, irrespective of tax consequences.

Appendix A—Common Types of Life Insurance

Life insurance can be categorized into two broad types: temporary (also called ''term'') insurance and permanent insurance. There are numerous variations of these products. However, most life insurance policies fall within one (or a combination) of the following categories.

Temporary (Term) Insurance

Temporary (term) insurance provides life insurance protection for a specified time period. Death benefits are payable only if the insured dies during the specified period. If a loss does not occur during the specified term, the policy lapses and provides no further protection. Term insurance premiums do not have a savings component; thus, term insurance does not create cash surrender value (CSV).

Permanent Insurance

In contrast to term insurance, permanent insurance is intended to provide life insurance protection for the entire life of the insured, and its premium structure includes a savings component. Permanent insurance policy premiums typically have two components: the insurance component (e.g., mortality cost, administrative fees, and sales loads) and the savings component. Mortality cost represents the cost imposed on the policyholder by the insurance company to cover the amount of pure insurance protection for which the insurance company is at risk.

The savings component typically is referred to as CSV. The policyholder may use the CSV to make the minimum premium payments necessary to maintain the death benefit protection and may access the CSV by taking out loans or making partial surrenders. If permanent insurance is surrendered before death, surrender charges may be assessed against the CSV. Generally, surrender charges are assessed if the policy is surrendered within the first 10 to 15 years.

Two broad categories of permanent insurance are:

- *Whole life.* A traditional form of permanent insurance designed so that fixed premiums are paid for the entire life of the insured. Death benefit protection is provided for the entire life of the insured, assuming all premiums are paid.
- *Universal life.* A form of permanent insurance designed to provide flexibility in premium payments and death benefit protection. The policyholder can pay maximum premiums and maintain a very high CSV. Alternatively, the policyholder can make minimal payments in an amount just large enough to cover mortality and other insurance charges.

Purposes for Which Institutions Commonly Purchase Life Insurance

Key person. Institutions often purchase life insurance to protect against the loss of ''key persons'' whose services are essential to the continuing success of the institution and whose untimely death would be disruptive. For example, an institution may purchase insurance on the life of an employee or director whose death would be of such consequence to the institution as to give it an insurable interest in his or her life. The determination of whether an individual is a key person does not turn on that individual's status as an officer or director, but on the nature of the individual's economic contribution to the institution.

The first step in indemnifying an institution against the loss of a key person is to identify the key person. The next and possibly most difficult step is estimating the insurable value of the key person or the potential loss of income or other value that the institution may incur from the untimely death of that person.

Because the most appropriate method for determining the value of a key person is dependent upon individual circumstances, the agencies have not established a formula or a specific process for estimating the value of a key person. Instead, the agencies expect institutions to consider and analyze all relevant factors and use their judgment to make a decision about the value of key persons.

Key-person life insurance should not be used in place of, and does not diminish the need for, adequate management-succession planning. Indeed, if an institution has an adequate management-succession plan, its reliance on a key person should decline as the person gets closer to retirement.

Financing or cost recovery for benefit plans. Like other businesses, institutions often use life insurance as a financing or cost-recovery vehicle for pre- and post-retirement employee benefits, such as individual or group life insurance, health insurance, dental insurance, vision insurance, tuition reimbursement, deferred compensation, and pension benefits.

Permanent insurance is used for this purpose. In these arrangements, an institution insures the lives of directors or employees in whom it has an insurable interest to reimburse the institution for the cost of employee benefits. The group of insured individuals may be different from the group that receives benefits. The institution's obligation to provide employee benefits is separate and distinct from the purchase of the life insurance. The life insurance purchased by the institution remains an asset even after the employer's relationship with an insured employee is terminated. The employees who receive benefits, whether insured or not, have no ownership interest in the insurance (other than their general claim against the institution's assets arising from the institution's obligation to provide the stated employee benefits).

There are two common methods of financing employee benefits through the purchase of life insurance. The first is the cost-recovery method, which usually involves present-value analysis. Typically, the institution projects the amount of the expected benefits owed to employees and then discounts this amount to determine the present value of the benefits. Then, the institution purchases a sufficient amount of life insurance on the lives of certain employees so that the gain (present value of the life insurance proceeds less the premium payments) from the insurance proceeds reimburses the institution for the benefit payments. Under this method, the institution absorbs the cost of providing the employee benefits and the cost of purchasing the life insurance. The institution holds the life insurance and collects the death benefit to reimburse the institution for the cost of the employee benefits and the insurance.

The second method of financing employee benefits is known as cost offset. With this method, the institution projects the annual employee benefit expense associated with the benefit plan. Then, the institution purchases life insurance on the lives of certain employees. The amount earned on the CSV each year should not exceed the annual benefit expense.

Split-dollar life insurance arrangements. Institutions sometimes use split-dollar life insurance arrangements to provide retirement benefits and death benefits to certain employees as part of their compensation. Under split-dollar arrangements, the employer and the employee share the rights to the policy's CSV and death benefits. The employer and the employee may also share premium payments. If the employer pays the entire premium, the employee may need to recognize taxable income each year in accordance with federal income tax regulations.

Split-dollar arrangements may be structured in a number of ways. The two most common types of split-dollar arrangements are:

- *Endorsement split-dollar.* The employer owns the policy and controls all rights of ownership. The employer provides the employee an endorsement of the portion of the death benefit specified in the plan agreement with the employee. The employee may designate a beneficiary for the designated portion of the death benefit. Under this arrangement, the employer typically holds the policy until the employee's death. At that time, the employee's beneficiary receives the designated portion of the death benefits, and the employer receives the remainder of the death benefits.
- *Collateral-assignment split-dollar.* The employee owns the policy and controls all rights of ownership. Under these arrangements, the employer usually pays the entire premium or a substantial part of the premium. The employee assigns a collateral interest in the policy to the employer that is equal to the employer's interest in the policy. The employer's interest in the policy is set forth in the split-dollar agreement between the employer and the employee. Upon retirement, the employee may have an option to buy the employer's interest in the insurance policy. This transfer of the employer's interest to the employee is typically referred to as a "roll-out." If a "roll-out" is not provided or exercised, the employer does not receive its interest in the policy until the employee's death.

Split-dollar life insurance is a very complex subject that can have unforeseen tax and legal consequences. Internal Revenue Service regulations issued in 2003[14] govern the taxation of

14. 68 *Fed. Reg.* 54336 (Sept. 17, 2003), chiefly codified at 26 CFR 1.61-22 and 1.7872-15.

split-dollar life insurance arrangements entered into or materially modified after September 17, 2003.[15] These rules provide less favorable tax treatment to split-dollar arrangements than existed previously. Institutions considering entering into a split-dollar life insurance arrangement should consult qualified tax, insurance, and legal advisers.

Life insurance on borrowers. State law generally recognizes that a lender has an insurable interest in the life of a borrower to the extent of the borrower's obligation to the lender. In some states, the lender's insurable interest may equal the borrower's obligation plus the cost of insurance and the time value of money. Institutions are permitted to protect themselves against the risk of loss from the death of a borrower. This protection may be provided through self-insurance, the purchase of debt-cancellation contracts, or by the purchase of life insurance policies on borrowers.

Institutions can take two approaches in purchasing life insurance on borrowers. First, an institution can purchase life insurance on an individual borrower for the purpose of protecting the institution specifically against loss arising from that borrower's death. Second, an institution may purchase life insurance on borrowers in a homogeneous group of loans employing a cost-recovery technique similar to that used in conjunction with employee benefit plans. Under this method, the institution insures the group of borrowers for the purpose of protecting the institution from loss arising from the death of any borrower in the homogeneous pool. Examples of homogeneous pools of loans include consumer loans that have distinctly similar characteristics, such as automobile loans, credit card loans, and residential real estate mortgages.

When purchasing insurance on an individual borrower, an institution should, given the facts and circumstances known at the time of the insurance purchase, make a reasonable effort to structure the insurance policy in a manner consistent with the expected repayment of the borrower's loan. To accomplish this, management should estimate the risk of loss over the life of the loan and match the anticipated insurance proceeds to the risk of loss. Generally, the risk of loss will be closely related to the outstanding principal of the debt. The insurance policy should be structured so that the expected insurance proceeds never substantially exceed the risk of loss.

When purchasing life insurance on borrowers in a homogeneous pool of loans, an institution's management should, given the facts and circumstances known at the time of the insurance purchase, make a reasonable effort to match the insurance proceeds on an aggregate basis to the total outstanding loan balances. If allowed by state law, institutions may match the insurance proceeds to the outstanding loan balances plus the cost of insurance on either a present-value or future-value basis. This relationship should be maintained throughout the duration of the program.

The purchase of life insurance on a borrower is not an appropriate mechanism for effecting a recovery on an obligation that has been charged off, or is expected to be charged off, for reasons other than the borrower's death. In the case of a charged-off loan, the purchase of life insurance on the borrower does not protect the institution from a risk of loss since the loss has already occurred. Therefore, the institution does not need to purchase insurance. Acquiring insurance that an institution does not need may subject the institution to unwarranted risks, which would be an unsafe and unsound banking practice. In the case of a loan that the institution expects to charge off for reasons other than the borrower's death, the risk of loss is so pronounced that the purchase of life insurance by the institution at that time would be purely speculative and an unsafe and unsound banking practice.

Internal Revenue Code section 264(f) disallows a portion of an institution's interest deduction for debt incurred to purchase life insurance on borrowers. Institutions considering the purchase of insurance on borrowers should consult their tax advisers to determine the economic viability of this strategy.

Life insurance as security for loans. Institutions sometimes take an interest in an existing life insurance policy as security for a loan. Institutions also make loans to individuals to purchase life insurance, taking a security interest in the policy, a practice known as "insurance-premium financing." As with any other type of lending, extensions of credit secured by life insurance should be made on terms that are consistent with safe and sound banking practices. For instance, the borrower should be obligated to repay the

15. Split-dollar arrangements entered into prior to September 17, 2003, and not materially modified thereafter may be treated differently.

loan according to an appropriate amortization schedule.

Generally, an institution may not rely on its security interest in a life insurance policy to extend credit on terms that excuse the borrower from making interest and principal payments during the life of the borrower with the result that the institution is repaid only when the policy matures upon the death of the insured. Lending on such terms is generally speculative and an unsafe and unsound banking practice.

Institutions may acquire ownership of life insurance policies for debts previously contracted (DPC) by invoking their security interest in a policy after a borrower defaults. Consistent with safety and soundness, institutions should use their best efforts to surrender or otherwise dispose of permanent life insurance acquired for DPC at the earliest reasonable opportunity.[16] In the case of temporary insurance acquired for DPC, retention until the next renewal date or the next premium date, whichever comes first, will be considered reasonable.

Appendix B—Glossary

Cash surrender value (CSV). The value available to the policyholder if the policy is surrendered. If no loans are outstanding, this amount is generally available in cash. If loans have been made, the amount available upon surrender is equal to the cash surrender value less the outstanding loan (including accrued interest).

Deferred acquisition costs (DAC). DAC represents the insurance carrier's up-front costs associated with issuing an insurance policy, including taxes and commissions and fees paid to agents for selling the policy. The carrier charges the policyholder for these costs. Carriers capitalize DAC and recover them in accordance with applicable tax law. As the carrier recovers DAC, it credits the amount to the policyholder.

Experience-rated pricing. A pricing method that bases prices for insurance products on the actual expenses and claims experience for the pool of individuals being insured.

General account. A design feature that is generally available to purchasers of whole or universal life insurance whereby the general assets of the insurance company support the policy's CSV.

Interest-crediting rate. The gross yield on the investment in the insurance policy, that is, the rate at which the cash value increases before considering any deductions for mortality cost, load charges, or other costs that are periodically charged against the policy's cash value.

There are a number of crediting rates, including "new money" and "portfolio." Using the "portfolio" crediting rate, the institution will earn a return based upon the existing yield of the insurance carrier's portfolio each year. Using the "new money" crediting rate, the institution will earn a return based upon yields available in the market at the time it purchases the policy.

Modified endowment contract (MEC). Type of policy that is defined in Internal Revenue Code section 7702A. A MEC generally involves the payment of a single premium at the inception of the contract; thus, it fails the so-called seven-pay test set forth in the statute. MECs are denied some of the favorable tax treatment usually accorded to life insurance. For example, most distributions, including loans, are treated as taxable income. An additional 10 percent penalty tax also is imposed on distributions in some circumstances. However, death benefits remain tax-free.

Mortality charge. The pure cost of the life insurance death benefit within a policy. It represents a cost to the purchaser and an income item to the carrier. Mortality charges retained by the insurance carrier are used to pay claims.

Mortality reserve. In separate-account products, the mortality reserve represents funds held by an insurance carrier outside of the separate account to provide for the payment of death benefits.

Non-MEC. An insurance contract that is not categorized as a MEC under Internal Revenue Code section 7702A.

Separate account. A separate account is a design feature that is generally available to purchasers of whole life or universal life whereby the policyholder's CSV is supported by assets segregated from the general assets of the carrier. Under such an arrangement, the policyholder

16. The OCC has generally directed national banks to surrender or divest permanent life insurance acquired for DPC within 90 days of obtaining control of the policy.

neither owns the underlying separate account nor controls investment decisions (e.g., timing of investments or credit selection) in the underlying separate account that is created by the insurance carrier on its behalf. Nevertheless, the policyholder assumes all investment and price risk.

Seven-pay test. The seven-pay test is a test set forth in Internal Revenue Code section 7702A that determines whether or not a life insurance product is a MEC for federal tax purposes.

Split-dollar life insurance. A split-dollar life insurance arrangement splits the policy's premium and policy benefits between two parties, usually an employer and employee. The two parties may share the premium costs while the policy is in effect, pursuant to a prearranged contractual agreement. At the death of the insured or the termination of the agreement, the parties split the policy benefits or proceeds in accordance with their agreement.

Stable value protection (SVP) contracts. In general, an SVP contract pays the policy owner of a separate account any shortfall between the fair value of the separate-account assets when the policy owner surrenders the policy and the cost basis of the separate account to the policy owner. The cost basis of the separate account typically would take into account the fair value of the assets in the account when the policy was initially purchased, the initial fair value of assets added to the account thereafter, interest credited to the account, the amount of certain redemptions and withdrawals from the account, and credit losses incurred on separate-account assets. Thus, SVP contracts mitigate price risk. SVP contracts are most often used in connection with fixed-income investments.

1035 exchange. A tax-free replacement of an insurance policy for another contract covering the same person(s) in accordance with section 1035 of the Internal Revenue Code.

Variable life insurance. Variable life insurance policies are investment-oriented life insurance policies that provide a return linked to an underlying portfolio of securities. The portfolio typically is a group of mutual funds chosen by the insurer and housed in a separate account, with the policyholder given some discretion in choosing among the available investment options.

Appendix C—Interagency Interpretations of the Interagency Statement on the Purchase and Risk Management of Life Insurance

The federal banking and thrift agencies developed responses to questions regarding the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance. A summary of these interpretations is included below to provide clarification on a wide variety of matters pertaining to financial reporting, credit-exposure limits, concentration limits, and the appropriate methodologies to use for calculating the amount of insurance an institution may purchase.

Legal Authority—State and Federal Law

As a general matter, the ability of state-chartered banks to purchase insurance (including equity-linked variable life insurance) is governed by state law. Section 24 of the Federal Deposit Insurance Act (the FDI Act) generally requires insured state-chartered banks to obtain the consent of the Federal Deposit Insurance Corporation (FDIC) before engaging as principal in activities (including making investments) that are not permissible for a national bank. Some state bank regulatory agencies have issued their own BOLI guidance or directives for their respective state-chartered institutions. A state-chartered institution should follow any BOLI guidance or directive issued by its state supervisory authority that is more restrictive than the interagency statement. Generally, if state law or policy is less restrictive than the interagency statement, a state-chartered institution should follow the interagency statement. If federal law is less restrictive than state law, a state-chartered institution should follow the state law.

Permissibility of Equity-Linked Securities in Separate-Account BOLI

The interagency statement states that national banks and federal savings associations may hold equity-linked variable life insurance policies (that is, insurance policies with a return tied to the performance of a portfolio of equity securities held in a separate account of the insurance company) only in very limited circumstances.

Similarly, state member banks may also hold equity-linked variable life insurance policies only in very limited circumstances. Because the range of instruments with equity-like characteristics varies significantly, the permissibility of each such instrument must be analyzed on a case-by-case basis. Furthermore, the agencies have significant concerns regarding whether an institution properly understands the complex risk profile that securities with "equity-like" characteristics often present. Some securities, even if legally permissible, may be inappropriate for the vast majority of financial institutions, whether held in an investment portfolio or a separate-account BOLI product. The agencies' April 1998 Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities provides guidance on the appropriateness of investments and risk-management expectations.

Senior Management and Board Oversight—Establishing BOLI Concentration Limits

Each institution should establish internal policies and procedures governing its BOLI holdings that limit the aggregate cash surrender value (CSV) of policies from any one insurance company as well as the aggregate CSV of policies from all insurance companies. The interagency statement is not intended to loosen the standards with respect to prior BOLI guidance. The agencies have rigorous expectations regarding the establishment of prudent limits and appropriate board and management oversight of the limit-setting process. Accordingly, exceptions will be subject to increased supervisory attention. The agencies continue to expect institutions to adopt per-carrier limits for BOLI, keeping in mind legal lending limits. Although the federal statutory and regulatory lending limits do not, as a general rule, impose a per-carrier legal constraint on BOLI because BOLI is not a loan, BOLI nevertheless does represent a long-term credit exposure. The agencies expect institutions to manage credit exposures in a prudent manner, irrespective of whether the exposure is subject to a statutory or regulatory limit. If an institution establishes an aggregate limit for BOLI based upon its applicable capital concentration threshold, it would seldom be prudent to have its per-carrier limit equal to the aggregate limit. Apart from credit considerations, it is also important to diversify BOLI exposures in order to control transaction risks that may be associated with an individual carrier's policies.

Per-Carrier Limits

Institutions should establish a per-carrier limit for separate-account policies. Diversification among carriers reduces transaction risks. Institutions should also explicitly consider whether it is appropriate to combine general- and separate-account exposures from the same carrier for purposes of measuring exposure against internal limits. The agencies believe that institutions, based upon their risk tolerance and understanding of insurance risks, should determine for themselves whether to combine such policies. In this regard, the agencies note that separate-account policies also present general-account credit exposures. For example, deferred acquisition costs (DAC) and mortality reserves associated with separate-account policies are general obligations of the insurance carrier. Moreover, when the death of an insured occurs, the difference between the death benefit amount and the cash surrender value comes from the carrier's general account. Finally, the actual credit exposure under a BOLI policy may be many times greater than the carrying value of the policy currently recorded on the institution's balance sheet, given the typical relationship between CSV and policy death benefits. Institutions should keep these factors in mind when evaluating whether and, if so, how to aggregate general- and separate-account exposures for purposes of monitoring compliance with internal limits.

Legal Limits and Concentrations

When establishing internal CSV limits, an institution should consider its legal lending limit, the capital concentration thresholds, and any applicable state restrictions on BOLI holdings. The following are the agencies' capital concentration definitions:

- The FDIC uses 25 percent of tier 1 capital to measure a capital concentration.
- The other agencies use tier 1 capital plus the allowance for loan and lease losses (ALLL).

A state-chartered institution should be guided by the more restrictive of the applicable state and federal limitations and thresholds. For example, if a state defines BOLI as an extension of credit subject to a statutory or regulatory lending limit, or otherwise imposes a per-carrier limit on BOLI, then institutions subject to that state's jurisdiction should ensure that their BOLI exposure to an individual carrier does not exceed the applicable state limit.

Permissibility of Holding Life Insurance on Former Employees and Former Key Persons

A well-managed institution adequately documents the purpose for which it is acquiring BOLI, as part of its pre-purchase analysis. When an institution purchases life insurance on a group of employees (whether it is a group policy or a series of individual policies) as a means to finance or recover the cost of employee benefits, and one or more of the insured employees is no longer employed by the bank, the insurance coverage may be retained by the institution provided—

- the application of the cost-recovery or cost-offset method (see "Quantifying the Amount of Insurance Appropriate for the Institution's Objectives" below) indicates that the amount of insurance held is not in excess of the amount required to recover or offset the cost of the institution's employee benefits,
- the policy is not specifically designated to cover only loss of income to the banking organization that may arise from the death of the employee,
- the coverage continues to qualify as an insurable interest under applicable state law, and
- the insurance asset continues to be a permissible holding under applicable state law for state-chartered institutions.

Additionally, if the policy no longer qualifies as insurance under the applicable state insurable-interest law, the policy may no longer be eligible for favorable tax treatment. These conditions apply to "benefits BOLI" despite the fact that the former employee was a "key person."

This is in contrast to true key-person insurance, in which the institution purchases life insurance on a key person in order to protect itself from financial loss in the event of that person's death. The interagency statement provides that a national bank or federal savings association may be required to surrender or otherwise dispose of key-person life insurance held on an individual who is no longer a key person because the institution will no longer suffer a financial loss from the death of that person. However, when an individual upon whom key-person life insurance has been held is no longer a key person, an institution may be able to recharacterize its objective for the insurance policy as recovery of the cost of providing employee benefits. In such cases, the institution must demonstrate, through appropriate analysis and quantification, that the insurance coverage satisfies the retention conditions, as set forth in the preceding paragraph. For a state-chartered institution, the recharacterization and retention of such key-person life insurance must be permissible under applicable state law. In circumstances where a national bank or federal savings association would be required to surrender or otherwise dispose of key-person life insurance, a state-chartered institution must also surrender or otherwise dispose of a key-person policy unless the retention of the policy is permitted under applicable state law and the institution obtains the FDIC's consent to continue to hold the policy under section 24 or section 28 of the FDI Act, as appropriate.

Quantifying the Amount of Insurance Appropriate for the Institution's Objectives

Institutions are responsible for ensuring that they do not purchase excessive amounts of insurance coverage on their employees relative to salaries paid and the costs of benefits to recover. Examiners will evaluate an institution's BOLI holdings and make a supervisory judgment as to whether insurance amounts on employees are so excessive as to constitute speculation or an unsafe or unsound practice on a case-by-case basis, as they do for other aspects of an institution's operations. Such an evaluation would be based on the totality of the circumstances.

Institutions may use either the cost-recovery or cost-offset method to quantify the amount of insurance permissible for purchase to finance or recover employee benefit costs. When using the cost-offset approach, an institution must ensure that the projected increase in CSV each year

over the expected duration of the BOLI is less than or equal to the expected employee benefit expense for that year. When using the cost-recovery method, regardless of an institution's quantification method, management must be able to support, with objective evidence, the reasonableness of all assumptions used in determining the appropriate amount of insurance coverage needed, including the rationale for its discount rates (when the cost-recovery method is used) and cost projections.

Applicability of Prior Guidance for Split-Dollar Arrangements

The pre-purchase analysis guidance in the interagency statement applies to life insurance policies used in split-dollar arrangements that are acquired after December 7, 2004. The guidance concerning the ongoing risk management of life insurance after its purchase applies to life insurance policies, including those used in split-dollar arrangements, regardless of when acquired.

The FDIC's prior guidance on split-dollar arrangements, which was included in supervisory guidance on BOLI that was issued in 1993, has been superseded; until the issuance of the interagency statement, the FDIC had generally followed the Office of the Comptroller of the Currency's prior guidelines from 2000. Otherwise, the prior guidance issued by the agencies on split-dollar life insurance remains in effect. Each agency issued the interagency statement under its own bulletin, letter, or notice. For example, the Federal Reserve Board's issuance of the interagency statement is cross-referenced in SR-04-19, and the prior guidance on split-dollar life insurance arrangements is not superseded.

Accounting Considerations

An institution may purchase multiple permanent insurance policies from the same insurance carrier, with each policy having its own surrender charges. In some cases, the insurance carrier will issue a rider or other contractual provision stating that it will waive the surrender charges if all of the policies are surrendered at the same time. Because it is not known at any balance-sheet date whether one or more of the policies will be surrendered before the deaths of the insureds, the possibility that the institution will surrender all of these policies simultaneously and avoid the surrender charges is a gain contingency. This guidance should be applied to all insurance policies held by an institution regardless of when they were acquired. Therefore, an institution that has purchased BOLI is required to report the CSV on the bank's balance sheet net of the surrender charges (even if the policies have been in force for some time and the institution's auditors have not previously required reporting the CSV net of the surrender charges).

Based on the agencies' review of FASB Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance" (TB 85-4), including its appendix, the agencies believe that TB 85-4 is intended to be applied on a policy-by-policy basis. It, therefore, does not permit the aggregation of multiple separate policies for balance-sheet-measurement purposes. Accordingly, the agencies do not intend to defer to institutions or their auditors on this issue. As of the balance-sheet date, an institution should determine the amount that could be realized under each separate insurance policy on a stand-alone basis without regard to the existence of other insurance policies or riders covering multiple policies. If a single insurance policy covers more than one individual, the realizable amount of the entire policy should be determined. A single insurance policy covering multiple individuals should not be subdivided into hypothetical separate policies for each covered individual, even if the carrier reports CSVs for each covered individual.

If a change in an institution's accounting for its holdings of life insurance is necessary for regulatory reporting purposes, the institution should follow Accounting Principles Board Opinion No. 20, "Accounting Changes"(APB 20).[17] APB 20 defines various types of accounting changes and addresses the reporting of corrections of errors in previously issued financial statements. APB 20 states that "[e]rrors in financial statements result from mathematical mistakes, mistakes in the application of accounting principles, or oversight or misuse of facts that existed at the time the financial statements were prepared."

17. Effective December 15, 2005, APB 20 will be replaced by FASB Statement No. 154, "Accounting Changes and Error Corrections—A replacement of APB Opinion No. 20 and FASB Statement No. 3."

For regulatory reporting purposes, an institution must determine whether the reason for a change in its accounting for its holdings of life insurance meets the APB 20 definition of an accounting error. If the reason for the change meets this definition and the amount is material, the error should be reported as a prior-period adjustment in the institution's regulatory reports. Otherwise, the effect of the correction of the error should be reported in current earnings. If the effect of the correction of the error is material, the institution should also consult with its primary federal regulatory agency to determine whether any previously filed regulatory reports should be amended. For the Call Report, the institution should report the amount of the adjustment in Schedule RI-A, item 2, "Restatements due to corrections of material accounting errors and changes in accounting principles," with an explanation in Schedule RI-E, item 4. The effect of the correction of the error on income and expenses since the beginning of the period in which the correction of prior-period earnings is reported should be reflected in each affected income and expense account on a year-to-date basis in the Call Report Income Statement (Schedule RI), not as a direct adjustment to retained earnings.

Rate of Return to the Bank in Split-Dollar Insurance Arrangements

The agencies would consider the institution's economic interest in a split-dollar life insurance arrangement policy, at a minimum, to be a return of the premiums paid plus a reasonable rate of return. The agencies would generally consider a reasonable rate of return to be one that provides the bank a return that is commensurate with alternative investments having similar risk characteristics (including credit quality and term) at the time in which the bank enters into the split-dollar arrangement. The rate of return is to be calculated net of any payments made (or to be made) from insurance proceeds to the employee's beneficiaries.

The agencies look at the economic value of compensation arrangements when determining the reasonableness of split-dollar compensation, but the agencies do not rely solely on income tax rules for determining this economic value. Other factors that the agencies might consider include, but are not limited to, the benefit of a split-dollar arrangement to the employee as a percentage of salary and the expected length of time until the institution recovers its invested funds.

1. To determine the level and direction of risk that purchases and holdings of life insurance pose to the state member bank, and to recommend corrective action, as appropriate.
2. To perform—
   a. a risk assessment that summarizes the level of inherent risk by risk category, and
   b. an assessment of the adequacy of the board of directors' and management's oversight of the activity, including an assessment of the bank's internal control framework.
3. To ensure that the risk assessment considers a state member bank's purchase and risk management of its—
   a. broad bank-owned life insurance (BOLI) programs, in which life insurance is purchased on a group of employees to offset employee benefit programs and the bank is the beneficiary;
   b. split-dollar insurance arrangements for individual (usually senior-level) bank employees; and
   c. holdings of key-person insurance.
4. Recognizing that management may not be as familiar with insurance products as it is with more-traditional bank products, to adequately identify and assess the risks of BOLI, as well as the risk exposures that may arise from purchases and holdings of life insurance.[1]
5. To apply a forward-looking approach to the review of a bank's purchase and risk management of life insurance, recognizing that the bank may be exposed to increasing operational risks as a result of its large purchases or holdings of this product. These risks may arise from—
   a. separate-account assets that contain holdings of complex equity-linked notes and derivative products;
   b. the growing use of guaranteed minimum death benefits and other complex guarantee structures, which may increase the operational risk to banks purchasing significant amounts of life insurance; and
   c. the potential losses that could result from—
      - inadequate recordkeeping, which may be related to tracking the potentially large variety of contracts and agreements and the potentially large number of insured current and former employees covered by the contracts, and
      - a failure to ensure that contract agreements between the insurance company, the vendor(s), and the employees are properly executed and honored.

1. As noted in more depth in section 4042.1, the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance, these risks include operational, liquidity, credit, legal, and reputational risk. Operational risk arises in part from the vast array of new life insurance products and structures being offered and from the complexity of tax considerations related to the products, under various state insurable-interest and federal tax laws.

PRELIMINARY RISK ASSESSMENT

1. Consider the following, among other relevant criteria as appropriate, when determining whether to include the review of bank-owned life insurance (BOLI) in the examination scope:
   a. the volume, growth, and complexity of BOLI purchases and holdings
      - Consider the amount of the bank's BOLI holdings, measured by the total of their cash surrender values (CSVs) as a percentage of capital, and determine whether the resulting percentage is an asset concentration of capital. (For state member banks, the Federal Reserve has defined the capital base for determining this concentration threshold to be a percentage of tier 1 capital plus the allowance for loan and lease losses.) Determine whether the BOLI holdings have grown or declined significantly in recent years, when compared with the BOLI holdings of peer banks (consult the Federal Reserve System's intranet for applicable surveillance and monitoring data).
      - Obtain a breakout of the CSV of BOLI assets, as reported on the bank's balance sheet, including the amounts attributable to split-dollar insurance arrangements, general BOLI plans covering a group of employees to recover the cost of employee compensation and benefit programs, and the amount, if any, attributable to key-person insurance.
      - Obtain a listing of the amount of the bank's reimbursable premium payments under split-dollar life insurance arrangements and the amount receivable for these policies, which is to be booked as ''other assets'' on the bank's balance sheet.
      - Determine whether a portion of the CSV is in separate-account holdings of a life insurance company. If the bank has separate-account holdings, determine (1) the composition of the underlying separate-account assets and (2) if these assets constitute higher-risk investments, including equity-linked notes, mortgage-backed securities with significant interest-rate risk, or other investments entailing significant market risk.
      - Determine whether any of the life insurance policies are held in out-of-state trusts. If so, ascertain—
        — whether management and the board of directors can demonstrate that they have performed an independent legal analysis to ensure that the legal structure employed does not jeopardize the bank's insurable interest in the insurance policies or its access to the policy proceeds, as applicable; and
        — whether the trust arrangement inappropriately disadvantages the bank (for example, by permitting inappropriate investments or permitting the insured or the beneficiary to borrow against the policy holding in such a way that could jeopardize the bank's ability to recover amounts owed to it under the trust agreement).
   b. BOLI concentrations
      - Determine if there is a CSV concentration of life insurance to one carrier in excess of 25 percent that includes both separate-account and general-account BOLI holdings.
      - Determine if there are any market-risk concentrations within the underlying separate-account assets, including, for example, interest-sensitive fixed-income holdings.
      - Determine if there are any equity-linked notes or direct equity holdings in the separate accounts.
      - Determine if the bank holds any large-exposure life insurance policies on particular individuals. If so, determine if the policies are split-dollar arrangements and, if so—
        — whether the board or a board committee has evaluated the rea-

sonableness of the compensation as part of the employee's overall compensation package, and
— whether the board or a board committee has determined that the overall compensation is appropriate.

c. the appropriateness and recency of materials presented to the bank's board of directors concerning the bank's purchase and risk management of life insurance relative to its insurance purchases and holdings
d. the appropriateness and recency of audits and compliance reviews of the bank's purchases and risk management of life insurance
e. the overall financial condition of the bank, its supervisory rating, and any concerns or potential concerns about its liquidity

2. Depending upon the outcome of the preliminary risk assessment and other relevant factors, consider performing the following examination procedures.

OPERATIONAL-RISK ASSESSMENT

Senior Management and Board Oversight

1. Evaluate whether board and senior management oversight is effective and ensures that the bank's purchases and holdings of BOLI are consistent with safe and sound banking practices.
2. Determine whether the board of directors understands the complex risk characteristics of the bank's insurance holdings and the role of BOLI in the bank's overall business strategy.

Accounting Considerations

3. Determine if the bank's financial and regulatory reporting of its life insurance activities follows applicable generally accepted accounting principles (GAAP), including the following guidance:
   a. *Financial Accounting Standards Board (FASB) Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance" (TB 85-4).* Only the amount that can be realized under an insurance contract as of the balance-sheet date (that is, the CSV reported to the bank by the insurance carrier, less any applicable surrender charges not reflected by the insurance carrier in the reported CSV) is reported as an asset. Since there is no right of offset, a BOLI investment is reported as an asset separately from any deferred compensation liability, provided that it was not purchased in connection with a tax-qualified plan.
   b. *Call Report instructions.* The bank is required to report the carrying value of its BOLI holdings (CSV net of applicable surrender charges) as a component of "other assets" and to report the earnings on these holdings as "other noninterest income."
4. Verify that the bank's deferred compensation agreements were accounted for using the guidance in the February 11, 2004, Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance.
5. Verify that any accounts receivable that represent the bank's reimbursable life insurance premiums paid are recorded as unimpaired account receivables (for example, life insurance policies that are not impaired as a result of declining CSVs backing the obligations or employees borrowing against CSVs). (Impaired amounts should be expensed.)

Policies and Procedures

6. Assess the adequacy of the bank's policies and procedures governing its BOLI purchases and holdings, including its guidelines to limit the aggregate CSV of policies from one insurance company as well as limit the aggregate CSV of policies from all insurance companies.
7. Verify if the bank's board of directors or the board's designated committee approved BOLI purchases in excess of 25 percent of capital or in excess of any lower internal limit. (For state member banks, the Federal Reserve has defined the capital base for determining this concentration threshold to be a percentage of tier 1 capital plus the

allowance for loan and lease losses.)

8. Determine the reasonableness of the bank's internal limits and whether management and the board of directors have considered, before purchasing BOLI, the bank's legal lending limit, its applicable state and federal capital concentration threshold, and any other applicable state restrictions on BOLI.
9. For banks that may have other credit exposures to insurance companies, determine if the bank has considered the credit exposures arising from its BOLI purchases when assessing its overall credit exposure to a carrier and to the insurance industry.
10. Determine whether the bank's management has justified and analyzed the risks associated with a significant increase in the bank's BOLI holdings.
11. Determine if the bank has advised its board of directors of the existence of the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance and of the risks associated with BOLI.

Pre-Purchase Analysis

12. Ascertain whether the bank maintains adequate records of its pre-purchase analysis of BOLI.
13. Evaluate whether the bank's board of directors, or a designated board committee, and senior management understand the risks, rewards, and unique characteristics of BOLI.

Need for Insurance, Economic Benefits, and Appropriate Insurance Type

14. Determine whether the bank identified the specific risk of loss to which it is exposed or the specific costs to be recovered by the purchase of life insurance.
15. Determine whether the bank analyzed the costs and benefits of planned BOLI purchases.

Amount of Insurance Appropriate for the Institution's Objectives

16. Find out if the bank estimated the size of its employee benefit obligation or the risk of loss to be covered in order to ensure that the amount of BOLI purchased was not excessive in relation to this estimate and the associated product risks.
17. Determine whether management can support, with objective evidence, the reasonableness of all of the assumptions used in determining the appropriate amount of insurance coverage needed by the bank, including the rationale for its discount rates and cost projections.

Vendor Qualifications

18. Evaluate whether the bank's management assessed its own knowledge of insurance risks, the vendor's qualifications, the amount of resources the bank is willing to spend to administer and service the BOLI, and the vendor's ability to honor the long-term financial commitments associated with BOLI.

Characteristics of Available Insurance Products

19. Evaluate whether the bank's management has reviewed and understands the characteristics of the various life insurance products available and of the products it has acquired.
20. Ascertain if and how the bank's management reviewed and selected the life insurance product characteristics that best matched its objectives, needs, and risk tolerance. Ascertain whether management evaluated and documented, before the bank acquired BOLI, the risks of the variety and complexity of life insurance products considered, how the selected insurance product works, the variables that affect the product's performance, and the applicable tax and accounting treatments.
21. Determine whether the bank's management reviewed and documented its consideration of the types and design features of BOLI. Determine whether management reviewed and documented the negotiable features associated with a separate-account insurance product (for example, its investment options, terms, and conditions; the cost of stable value protection (SVP); deferred acquisition costs (DAC); and mortality options) and with any SVP provider that

may have been separately contracted by the insurance carrier.

22. Verify that the bank's management conducted a thorough review of life insurance policies before acquiring the policies. Ascertain if management determined how the accounting rules would apply to those policies and if it understood any ambiguous contract provisions, such as costs, charges, or reserves, that may affect the amount of a policy's CSV.

Tax and Insurable-Interest Implications

23. For the bank's pre-acquisition review of BOLI and its subsequent BOLI purchases, verify that the bank's management considered and documented its analysis of the financial impact of surrendering a policy (for example, any tax implications).
24. Verify that the bank's management obtained appropriate legal reviews. An appropriate legal review ensures that—
    a. the bank complies with applicable tax and state insurable-interest requirements, and
    b. the bank's insured amounts are *not* excessive (therefore, the bank is not involved in impermissible speculation or unsafe and unsound banking practices).

Carrier Selection

25. Find out if the bank (1) reviewed the BOLI product's design and pricing and the administrative services of the proposed carrier and (2) compared these services with those of other insurance carriers.
26. Ascertain whether the bank's management reviewed the selected carrier's ongoing long-term ability to commit to the BOLI product, as well as its credit ratings, general reputation, experience in the marketplace, and past performance.
27. Determine if the bank performed a credit analysis on the selected BOLI carriers and if the analysis was consistent with safe and sound banking practices for commercial lending.

Split-Dollar or Other Insurance Arrangements That Result in Additional Insured Employee Compensation

28. When a bank acquires insurance that permits a bank officer or employee to designate a beneficiary or provides the officer or employee with additional compensation, determine if the bank identified and quantified its total compensation objective. Determine if the bank ensured (1) that the acquired split-dollar life or other insurance arrangement was consistent with that objective, including when insurance compensation is combined with all other compensation being provided, and (2) that the total compensation was not excessive.
29. Verify that the bank and the insured have entered into a written agreement that specifically states the bank's rights, the insured individual's rights, and the rights of any other parties (trusts or beneficiaries) to the policy's CSV and death benefits.
30. Verify that the bank's shareholders and their family members (who are not bank officers, directors, or employees and who do not provide goods and services to the bank) do not receive compensation in the form of split-dollar life or other insurance coverage benefits.
31. Determine whether the bank's management has assessed the bank's ability to borrow against the CSV of its split-dollar life insurance policies, as well as the ability of other parties (whether an insured officer, employee, or noninstitution owner) to borrow against the policy CSV, without impairing the bank's financial interest in the policy proceeds. Determine also—
    a. if the bank can liquidate the policy in order to meet liquidity needs; or
    b. if the bank effects an early policy surrender (such as might occur if an employee terminates his or her employment), if the surrender would preclude the bank from recovering its premium payments and a market rate of return on the premiums invested.
32. Determine if and how management verified that the bank would be able to recover its premium payments plus a market rate of return on the premiums invested, after the payment of policy proceeds to the employee's beneficiary under the split-dollar arrangement.

Other Elements of Pre-Purchase Analysis

33. Ascertain whether the bank's management thoroughly evaluated all significant risks. Determine whether management has established procedures to identify, measure, monitor, and control those risks.
34. Find out if the bank, before acquiring BOLI, thoroughly analyzed its associated risks and benefits. As appropriate, determine whether the bank compared the risks of BOLI with those of alternative methods for recovering costs associated with the loss of key persons, providing pre- and post-retirement employee benefits, or providing additional employee compensation.

Post-Purchase Analysis

35. Find out if management reviewed at least annually the bank's life insurance purchases and holdings with the bank's board of directors.[1] Ascertain if the review included, at a minimum—
    a. a comprehensive assessment of the specific risks associated with the bank's permanent insurance acquisitions;
    b. an identification of the bank's employees who are or will be insured (for example, vice presidents and above, employees of a certain grade level, etc.);
    c. an assessment of death benefit amounts relative to employee salaries;
    d. a calculation of the percentage of insured persons still employed by the bank;
    e. an evaluation of the material changes to BOLI risk-management policies;
    f. an assessment of the effects of policy exchanges;
    g. an analysis of mortality performance and the impact on income;
    h. an evaluation of material findings from internal and external audits and independent risk-management reviews;
    i. an identification of the reason for, and the tax implications of, any policy surrenders; and
    j. a peer analysis of BOLI holdings.

LIQUIDITY-RISK ASSESSMENT

1. Find out if management, before the bank's purchase of permanent insurance, recognized the illiquid nature of the bank's acquisition of its permanent insurance products. Determine whether management ensured that the bank had the long-term financial flexibility to continue holding the insurance assets for their full term of expected use.
2. Determine if management, before the bank's purchase of permanent insurance, adequately considered the contractual arrangements and product types that limit product liquidity in order to best optimize the value of the bank's insurance assets and their possible future use as liquidity and funding sources. Contract provisions that should be considered include—
    a. 1035 exchange fees and "crawl-out restrictions,"
    b. provisions that would result in the product's categorization for federal tax purposes as a modified endowment contract (MEC) or a non-MEC contract, and
    c. SVP contract provisions that may limit the bank's ability to surrender a policy early or that would increase the cost of an early surrender.

REPUTATION-RISK ASSESSMENT

1. Ascertain whether the bank has taken steps, including obtaining written consent from its insured officers and employees, to reduce its reputation risk that may result from BOLI purchases.
2. Determine if the bank maintains appropriate documentation evidencing that it obtained a formal written consent from its insured officers and employees.
3. Find out what segment of the employee base the bank has insured (i.e., officers or non-officers) and if the bank has taken out very high death benefit policies on employees, including lower-level employees.

CREDIT-RISK ASSESSMENT

1. Determine if the bank's management con-

1. More-frequent reviews should be conducted if significant changes to the BOLI program are anticipated, such as additional purchases, a decline in the financial condition of the insurance carrier(s), anticipated policy surrenders, or changes in tax laws or interpretations that could have an impact on the performance of BOLI.

ducted an independent financial analysis of the insurance carrier before the bank's purchase of a life insurance policy.
   a. Ascertain if management continues to monitor the life insurance company's condition on an ongoing basis.
   b. Verify that the bank's credit-risk management function participated in the review and approval of insurance carriers.
2. Determine whether the bank considered its legal lending limit, its credit concentration guidelines (the aggregate exposures to individual insurance carriers and the life insurance industry, including other bank credit relationships, such as credit exposures involving loans and derivatives), and any state restrictions on BOLI holdings.
3. Determine whether the bank's credit analysis of its BOLI holdings evaluated whether the policies to be acquired were either separate-account or general-account policies.
   a. Find out whether the separate-account policies included an SVP contract to protect the bank (as a policyholder) from declines in the fair value of separate-account assets.
   b. Ascertain if the bank evaluated the insurance carrier's separately contracted SVP provider's repayment capacity.

MARKET-RISK ASSESSMENT

1. Determine whether management fully understood (before the bank purchased its separate-account products)—
   a. how the life insurance products expose the bank to interest-rate risk;
   b. the instruments governing the investment policy, as well as how the separate account is managed;
   c. the inherent risk of a separate account; and
   d. whether the bank's risk from the purchase of separate-account products was appropriate.
2. For general-account products, ascertain if management understands the interest-crediting option the bank chose when purchasing the insurance policy.
3. Find out if the bank has established and if it maintains appropriate monitoring and reporting systems for interest-rate fluctuations and their effect on separate-account assets.
4. Find out if the bank has acquired an SVP contract for its separate-account policy in order to reduce income-statement volatility. (SVP contracts protect against declines in value attributable to changes in interest rates; they do not cover default risk.)
5. If the bank has not purchased an SVP contract, determine if management has established and maintained monitoring and reporting systems that will recognize and respond to price fluctuations in the fair value of separate-account assets.
6. If the bank has purchased an equity-linked variable life insurance policy, determine whether it is characterized as an effective economic hedge against the bank's equity-linked obligations under its employee benefit plans. (An effective hedge exists when changes in the economic value of the liability or other risk exposure being hedged are matched by counterbalancing changes in the value of the hedging instruments. The economic hedging criteria for equity-linked insurance products lessen the effect of price risk because changes in the amount of the equity-linked liability are required to offset changes in the value of the separate-account assets.)
7. If the bank is purchasing or has purchased a separate-account insurance product involving equity securities, determine if the bank's management has performed further analysis that—
   a. compares the equity-linked liability being hedged and the equity securities in the separate account,
   b. determines a target range for the hedge-effectiveness ratio and establishes a method for measuring ongoing hedge effectiveness, and
   c. establishes a process for analyzing and reporting to management and the board of directors the effect of the hedge on the bank's earnings and capital ratios (both with and without the hedging transaction).

COMPLIANCE/LEGAL-RISK ASSESSMENT

1. Determine whether the bank's compliance

and audit functions have evaluated its compliance with applicable state insurable-interest and federal tax laws in order to protect the bank's earnings and capital from the loss of tax benefits or from the imposition of fines or penalties by regulatory authorities for violations of, or noncompliance with, laws, rulings, regulations, prescribed practices, and ethical standards.

2. When the bank owns separate-account BOLI, determine whether the bank has implemented and maintains internal control policies and procedures that adequately ensure that it does not take any action that might be interpreted as exercising "control" over separate-account assets.
3. Determine whether the bank split commissions between a vendor and the bank's own subsidiary or affiliate insurance agency when purchasing life insurance. If so, determine whether the bank's compliance function has assessed the bank's compliance with state and federal securities and insurance laws regarding fee and commission arrangements.
4. Ascertain whether the bank seeks and documents the advice of legal counsel when determining legal and regulatory issues, requirements, and concerns related to its potential purchase or ownership of BOLI.
5. For a general-account insurance product, determine if the bank has assigned a standard risk weight of 100 percent to the general-account asset.
6. For a BOLI separate-account product (when the bank uses the look-through approach to assign risk weights according to the risk-based capital rules)—
   a. review the bank's documentation, and determine if the bank adequately verified that the separate-account BOLI assets are protected from the insurance company's general creditors in the event of the insurance company's insolvency;
   b. determine if the standard risk weight of 100 percent was assigned to the bank's BOLI assets when the bank's documentation is inadequate or does not exist;
   c. verify that a 100 percent risk weight has been assigned to (1) the portion of the bank's insurance asset that represents general-account claims on the insurer (such as DAC and mortality reserves that are realizable on the balance-sheet date) and (2) any portion of the carrying value attributable to an SVP contract (or if the SVP provider is not an insurance company, verify that the correct risk weight has been assigned for that obligor); and
   d. if the bank used a pro rata approach to risk-weighting the carrying value of a qualifying separate-account policy—
      - verify that the risk weight is applied to the separate account based on the most risky portfolio that could be held by the separate account (as stated in the investment agreement), except for any portions of the carrying value that are general-account claims attributable to either DAC or an SVP (which are generally risk-weighted at 100 percent);
      - verify that in no case may the assigned risk weight for the bank's entire separate-account holding be less than 20 percent; and
      - when the sum of the permitted investments across market sectors in the investment agreement is greater than 100 percent, determine if the bank assigned the highest risk weight for the maximum amount permitted in that asset class, and then applied the next-highest risk weights to the other asset classes until the aggregate of the permitted amounts equals 100 percent.

Purchase and Risk Management of Life Insurance

Internal Control Questionnaire

Effective date May 2006

Section 4042.4

Examiners should use only those internal control questions that are appropriate, given the size, complexity, and growth of a bank's bank-owned life insurance (BOLI) holdings.

PRELIMINARY RISK ASSESSMENT

1. Have the steps for conducting a preliminary risk assessment been followed, as they are set forth in section 4042.3? Have other relevant factors been considered to determine if further examination review may be warranted, in accordance with risk-focused supervision guidelines?
2. What particular factors have been identified to warrant a review of the bank's purchases and risk management of life insurance?

OPERATIONAL-RISK ASSESSMENT

Senior Management and Board of Directors Oversight

1. Has senior management and the board of directors initiated and maintained effective oversight of the bank's BOLI by—
   a. performing a thorough pre-purchase analysis of its risks and rewards and a post-purchase risk assessment?
   b. determining the permissibility of the bank's BOLI purchases and holdings under both the applicable state and federal requirements (whichever requirements are more restrictive)?
   c. determining the types and kinds of risks that are associated with BOLI?
   d. ascertaining and reviewing the safety-and-soundness considerations associated with the bank's BOLI?
   e. understanding the complex risk characteristics of the bank's insurance holdings and what role BOLI is to play in the bank's overall business?
2. Does the bank have a comprehensive risk-management process for purchasing and holding BOLI?

Accounting Considerations

3. When accounting for its holdings of life insurance, did the bank follow the guidance in FASB's Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance"? Are the bank's insurance policies reported on its balance sheet on the basis of each policy's cash surrender value (CSV), less any applicable surrender charges that are not reflected in the reported CSV?
4. On the bank's Call Report, did the bank's management —
   a. report the carrying value of its BOLI holdings as an "other asset"?
   b. report the earnings on the bank's holdings as "other noninterest income"?
   c. report the CSV separately, as required if the CSV amount exceeded the reporting threshold?
   d. expense only the noninvestment portion of the premium, in the case of bank-owned policies?
   e. expense the premium for employee-owned insurance purchased by the bank and record a receivable in "other assets" for any portion of the premium to be reimbursed to the bank under a contractual agreement?
5. Were the bank's deferred compensation agreements accounted for using the guidance in the February 11, 2004, Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance?

Policies and Procedures

6. Does the bank have comprehensive policies and procedures, including guidelines, that limit the aggregate CSV of policies from any one insurance company, as well as the aggregate CSV of policies from all insurance companies?
   a. Does the board of directors or a designated board committee require senior management to provide adequate and appropriate justification for establishing or revising internal CSV limits on the amount of BOLI the bank holds? Does

this justification take into account the bank's legal lending limits, its capital and credit concentration threshold, and any applicable laws and regulations?

b. Is written justification required when the amount of the bank's BOLI holdings approaches or exceeds 25 percent of the bank's capital (tier 1 capital plus the allowance for loan and lease losses)? Does the board of directors or a board committee approve this justification?

Pre-Purchase Analysis

7. Did the bank's management perform a written pre-purchase analysis of its BOLI products?
8. Did management identify the bank's need for BOLI, the appropriate type of insurance to be acquired, and the economic benefits to be derived from the purchase of BOLI? Did this analysis accomplish the following:
   a. identify the specific risk of loss to be covered by the insurance, or the costs the insurance is supposed to cover?
   b. determine what type BOLI (for example, general- or separate-account) and what BOLI features are needed, before acquiring the product?
   c. evaluate the permissibility and market risk of any underlying separate-account asset holdings, if separate-account BOLI is held?
   d. analyze projected policy values (CSV and death benefits) using various interest-crediting rates and mortality cost assumptions?
   e. estimate the size of the employee benefit obligation or the risk of loss to be covered? Did management ensure that the amount of BOLI coverage was appropriate for the bank's objectives and that BOLI was not excessive in relation to this estimate and the associated product risks?
   f. review the range of assumptions? Was management able to justify the assumptions with objective evidence, and deem them reasonable in view of previous and expected market conditions?
   g. assess whether the present value of the BOLI's expected future cash flows (net of the costs of the insurance) is less than the estimated present value of the expected after-tax employee benefit costs, when the bank uses BOLI to recover the costs of providing employee benefits?
9. Did the bank's management —
   a. review and assess its own knowledge of insurance risks, the vendor's qualifications, and the amount of the bank's resources that will be needed to administer and service the BOLI?
   b. demonstrate its familiarity with the technical details of the bank's insurance assets, and is management able to explain the reasons for and the risks associated with the product design features that have been selected?
   c. make appropriate inquiries to determine whether the vendor has the financial ability to honor its long-term commitments over an extended period of time?
   d. assure itself of the vendor's commitment to investing in the operational infrastructure that is necessary to support the BOLI?
   e. undertake its own independent review and not rely solely on prepackaged, vendor-supplied compliance information (such reliance is a potential cause for supervisory action)?
   f. properly evaluate the characteristics of the available insurance products against the bank's objectives, needs, and risk tolerance?
   g. determine if the bank's need for insurance on key persons or on a borrower's loan resulted in a matching of the maturity of the term or declining term insurance to the key person's expected tenure or the maturity of the borrower's loan?
   h. conduct a review of the insurance carrier that included—
      - a credit analysis of the potential insurance carrier (the analysis should have been performed in a manner consistent with safe and sound banking practices for commercial lending)?
      - a review of the bank's needs and a comparison of those needs with the proposed carrier's product design, pricing, and administrative services?
      - a review of the insurance carrier's commitment to the BOLI product, as well as the carrier's general reputation, experience in the marketplace, and past performance?

i. determine whether the total amount of compensation and insurance to be provided to an employee is excessive, if the purchased BOLI will result in the payment of additional compensation?
j. analyze the associated significant credit risks and the bank's ability to monitor and respond to those risks?
k. as appropriate, analyze the risks and benefits of BOLI, compared with other available methods for recovering costs associated with the loss of key persons, providing pre- and post-retirement employee benefits, or providing additional employee compensation?
l. sufficiently document its comprehensive pre-purchase analysis (including its analysis of both the types and product designs of purchased BOLI and the bank's overall level of BOLI holdings)?

Post-Purchase Analysis

10. Do management and the board of directors annually review the performance of the bank's insurance assets? Does the annual review include—
    a. a comprehensive assessment of the specific risks associated with permanent insurance acquisitions?
    b. an identification of employees who are or will be insured (e.g., vice presidents and above, employees of a certain grade level)?
    c. an assessment of death benefit amounts relative to employee salaries?
    d. a calculation of the percentage of insured persons still employed by the institution?
    e. an evaluation of the material changes to BOLI risk-management policies?
    f. an assessment of the effects of policy exchanges?
    g. an analysis of mortality performance and the impact on income?
    h. an evaluation of material findings from internal and external audits and independent risk-management reviews?
    i. an identification of the reason for and the tax implications of any policy surrenders?
    j. a peer analysis of BOLI holdings?

Tax and Insurable-Interest Implications

11. Has the bank's management explicitly considered the financial impact (for example, the tax provisions and penalties) of surrendering a BOLI policy?
12. Does the bank's management have or has it obtained appropriate legal review to ensure that it will be in compliance with applicable tax and state insurable-interest requirements? Is management aware of the relevant tax features of the insurance assets, including whether the bank's purchase would—
    a. make the bank subject to the alternative minimum tax?
    b. jeopardize the tax-advantaged status of the bank's insurance holdings?
    c. qualify (under applicable state law) an insurable ownership interest in the BOLI policy covering the bank's officers or its employees (including any applicable state law pertaining to the insured's consent and the amounts of allowable insurance coverage for an employee)?
13. Did the bank establish an out-of-state trust to hold its BOLI assets, and, if so, has the bank adequately assessed its insurable interest, given the arrangement?

LIQUIDITY-RISK ASSESSMENT

1. Has the bank's management fully recognized and considered the illiquid nature of the BOLI to be acquired? (An institution's BOLI holdings should be considered when assessing liquidity and assigning the component rating for liquidity.)
2. Did management determine if the bank has the long-term financial flexibility to hold the insurance asset for the full term of its expected use?

REPUTATION-RISK ASSESSMENT

1. Has the bank's management implemented procedures to ensure that the bank maintains appropriate documentation that evidences employees' informed consent for the bank's purchase of insurance on their lives? Do these procedures ensure that the bank

obtains employees' explicit consent before purchasing the insurance?

2. Has the bank obtained insurance products that insure large segments of its employee base (including the bank's non-officers)? Do these policies provide very high death benefits on employees, possibly causing the bank to be exposed to increased reputation risk if explicit consent was not obtained from the employees?

CREDIT-RISK ASSESSMENT

1. Did the bank's management conduct an independent financial analysis of the insurance carrier before purchasing the life insurance policy?
   a. Does management continue to monitor the life insurance company's financial condition on an ongoing basis?
   b. Did the bank's credit-risk management function participate in the review and approval of insurance carriers?
2. When establishing exposure limits for aggregate BOLI holdings and exposures to individual carriers, did the bank's management consider—
   a. the bank's legal lending limit?
   b. the applicable state and federal credit concentration exposure guidelines?
   c. the aggregate CSV exposures as a percentage of the bank's capital?
3. Has the bank's credit-risk management process taken into account credit exposures arising from both BOLI holdings and other credit exposures (loans, derivatives, and other insurance products) when measuring exposures to individual carriers?
4. Did the bank's credit analysis of its BOLI holdings consider whether the policies to be acquired were separate-account or general-account policies?
   a. For the separate-account policies, did the credit review include a risk analysis of the underlying separate-account assets?
   b. For separate-account policies that include a stable value protection (SVP) contract, has the repayment capacity of the insurance carrier's separately contracted SVP providers been evaluated?

MARKET-RISK ASSESSMENT

1. Did management adequately assess the interest-rate risk exposure of BOLI before purchasing the products for separate-account and general-account assets?
2. Has the bank's management reviewed, and does it understand the instruments governing the separate-account investment policy and its management?
   a. Does the bank's management understand the risk inherent within the separate account?
   b. Has the bank's management determined if the risk is appropriate?
3. Have monitoring and reporting systems been established that will enable the bank's management to monitor, measure, and appropriately manage interest-rate risk exposure from BOLI holdings when assessing the bank's overall sensitivity to interest-rate risk?

COMPLIANCE/LEGAL-RISK ASSESSMENT

1. Has the bank's audit and/or compliance function reviewed the bank's legal and regulatory requirements as they pertain to life insurance holdings? Did the review consider—
   a. state insurable-interest laws?
   b. the Employee Retirement Income Security Act of 1974 (ERISA)?
   c. the Federal Reserve Board's Regulation W (12 CFR 223)?
   d. applicable federal prohibitions on insider loans, including the Federal Reserve Board's Regulation O, that may apply to split-dollar life insurance arrangements?
   e. the interagency guidelines for establishing standards for safety and soundness?[1]
   f. other state and federal regulations applicable to BOLI?
2. To ensure that the life insurance qualifies for its tax-advantaged status, has the bank's management implemented and maintained internal policies and procedures to ensure that "control" will not be exercised over any of the separate-account assets, espe-

1. For state member banks, see 12 CFR 208, appendix D-1.

cially those involving privately placed policies?

3. Does the bank's board of directors, its designated board committee, and its management seek the assistance of legal counsel when determining the legal and regulatory issues related to the acquisition and holding of life insurance policies?
4. Has management thoroughly reviewed, and does it understand, the instruments governing the investment policy and the management of a separate account, before purchasing a separate-account policy?
5. If the bank has not purchased SVP for a separate-account BOLI policy, has management established the appropriate monitoring and reporting systems that will enable it to recognize and respond to price fluctuations in the fair value of the separate-account assets?
6. When the bank considers or purchases a separate-account BOLI product involving equity securities, does it analyze the equity securities? Does this analysis—
   a. compare the specific equity-linked liability being hedged against the securities held in a separate account?
   b. establish a target ratio for hedge effectiveness, as well as a method for measuring hedge effectiveness on an ongoing basis?
   c. establish a process for analyzing and reporting to the board of directors, its designated committee, and senior management the effect of the hedge on the bank's earnings and capital ratios (this analysis should include a consideration of the results both with and without the hedging transaction)?
7. When reporting its risk-based capital, has the bank ensured that it accurately calculates and reports its risk-weighted assets for BOLI holdings according to the risk-based capital guidelines and the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance (see section 4042.1 and SR-04-19 and its attachment)?
   a. For a general-account insurance product, has the bank applied a standard risk weight of 100 percent to the general-account asset?
   b. When the bank has applied a look-through approach for separate-account holdings—
      - has management determined if BOLI assets would be protected from the insurance company's general creditors in the event of its insolvency? Has the bank documented its assessment that BOLI assets are protected?
      - has the portion of the carrying value of the separate-account policy (that reflects the amounts attributable to the insurer's DAC and mortality reserves, and any other portion that is attributable to the carrying value of an SVP contract) been risk-weighted using the 100 percent risk weight applicable to the insurer's general-account obligations? Or, if the SVP provider is not an insurance company, has the portion of the carrying value been risk-weighted as appropriate for that obligor?
8. When the bank has used a pro rata approach to risk-weighting the carrying value of a qualifying separate-account policy, did it use the appropriate procedures, as outlined in the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance (see section 4042.1 and SR-04-19 and its attachment)?
   a. Has the bank ensured that its assigned aggregate risk weight for all separate-account BOLI holdings will be 20 percent or more?
   b. When the sum of the permitted investments across market sectors in the investment agreement is greater than 100 percent, was the highest risk weight applied for the maximum amount permitted in that asset class, and was the next-highest risk weight then applied until the cumulative permitted amounts equal 100 percent?

Banking organizations have long been engaged in the sale of insurance products and annuities, although these activities historically have been subject to several restrictions. For example, until recently, national banks could sell most types of insurance, but only through an agency located in a small town. Bank holding companies also were permitted to engage in only limited insurance agency activities under the Bank Holding Company Act. State-chartered banks, on the other hand, generally have been permitted to engage in insurance sales activities as agents to the extent permitted by state law.

The Gramm-Leach-Bliley Act of 1999 (the GLB Act), however, authorized national banks and state-chartered member banks to sell all types of insurance products through a financial subsidiary. *The GLB Act generally did not change the powers of banks to sell insurance directly.* As a result of the GLB Act and marketplace developments, many banking organizations are increasing the range and volume of their insurance and annuities sales activities. To the extent permitted by applicable law, banking organizations may conduct insurance and annuity sales activities through a variety of structures and delivery channels, including ownership of an insurance underwriter or an insurance agency or broker, the employment by a bank of licensed agents, a joint marketing arrangement with a producer,[1] independent agents located at a bank's office, direct mail, telemarketing, and Internet marketing.

A banking organization may also conduct insurance or annuity sales activities through a managing general agent (MGA). An MGA is a wholesaler of insurance products and services to insurance agents. The MGA has a contractual agreement with an insurance carrier to assume functions for the carrier, which may include marketing, accounting, data processing, policy recordkeeping, and monitoring or processing claims. The MGA may rely on various local agents or agencies to sell the carrier's products. Most states require an MGA to be licensed.

OVERVIEW AND SCOPE

The following guidance pertains to state member banks that are either directly or indirectly engaged in the sale of insurance or annuity products. Examiner guidance on performing appropriate risk assessments of a state member bank's insurance and annuity sales activities is included.[2] Additionally, guidance is provided for examining a state member bank's compliance with the consumer protection rules relating to insurance and annuities sales activities that are contained in the Board's December 2000 revisions to Regulation H (subpart H) (12 CFR 208.81–86), "Consumer Protection in Sales of Insurance" (CPSI). Subpart H, which became effective on October 1, 2001, implements the consumer protection requirements of the GLB Act, which are codified at 12 USC 1831x. (See 65 *Fed. Reg.* 75841, December 4, 2000.) The regulation applies not only to the sale of insurance products or annuities by the bank, but also to activities of any person engaged in insurance product or annuity sales on behalf of the bank, as discussed in this guidance. The guidance is generally not applicable to debt-cancellation contracts and debt-suspension agreements, unless these products are considered to be insurance products by the state in which the sales activities are conducted.

The GLB Act permits state member banks that are not authorized by applicable state law to sell insurance directly to do so through a financial subsidiary.[3] A financial subsidiary engaged in insurance sales may be located wherever state

1. The term "producer" refers broadly to persons, partnerships, associations, limited liability corporations, etc., that hold a license to sell or solicit contracts of insurance to the public. Insurance agents and agencies are producers who, through a written contractual arrangement known as a direct appointment, represent one or more insurance underwriters. Independent agents and agencies are those producers that sell products underwritten by one or more insurance underwriters. Captive agents and agencies represent a specific underwriter and sell only its products. Brokers are producers that represent the purchaser of insurance and obtain bids from competing underwriters on behalf of their clients. State insurance laws and regulations often distinguish between an insurance agent and a broker; in practice, the terms are often used interchangeably.

2. The term "risk assessment" denotes the work product described in SR-97-24, "Risk-Focused Framework for Supervision of Large Complex Institutions," and entails an analysis of (1) the level of inherent risk by type of risk (operational, legal, market, liquidity, credit, and reputation risk) for a business line or business function, (2) the adequacy of management controls over that business line or business function, and (3) the direction of the risk (increasing, decreasing, or stable).

3. Rules pertaining to state member bank financial subsid-

law permits the establishment and operation of an insurance agency. Such subsidiaries, however, would be subject to state licensing and other requirements.

The Federal Reserve is responsible for evaluating the consolidated risk profile of a state member bank. This reponsibility includes determining the risks posed to the state member bank from the insurance and annuity sales activities it conducts directly or indirectly, as well as determining the effectiveness of the bank's risk-management systems. However, the GLB Act also established a regulatory framework that is designed to ensure that the Federal Reserve coordinates with, and relies to the extent possible on information from, the state insurance authorities when it is supervising the insurance activities a state member bank conducts through a functionally regulated subsidiary.

Consistent with the Federal Reserve's risk-focused framework for supervising banking organizations, resources allocated to the review of insurance sales activities should be commensurate with the significance of the activities and the risk they pose to the bank. The scope of the review depends on the significance of the activity to the state member bank and the extent to which the bank is directly involved in the activity. Examiner judgment is required to tailor the reviews, as appropriate, on the basis of the legal, organizational, and risk-management structure of the state member bank's insurance and annuity sales activities and on other relevant factors.[4]

SUPERVISORY APPROACH FOR THE REVIEW OF INSURANCE AND ANNUITY SALES ACTIVITIES

Supervisory Objective

The primary objective for the review of a state member bank's insurance and annuity sales activities is to determine the level and direction of risk such activities pose to the state member bank. The review includes insurance and annuity sales activities the state member bank conducts directly (by or in conjunction with a subsidiary or affiliate) or through a third-party arrangement. Primary risks that may arise from insurance sales activities include operational, legal, and reputational risk. If the state member bank does not adequately manage these risks, they could have an adverse impact on its earnings and capital. The examiner should produce (1) a risk assessment that summarizes the level of inherent risk to the state member bank by risk category and (2) an assessment of the adequacy of board of directors' and management oversight of the insurance and annuity sales activities, including their internal control framework. For those state member banks selling insurance or annuity products, or that enter into arrangements under which another party sells insurance or annuity products at the bank's offices or on behalf of the bank, a second objective of the review is to determine the bank's compliance with the consumer protection provisions of the GLB Act and the CPSI regulation.

State Regulation of Insurance Activities

Historically, insurance activities have primarily been regulated by the states. In 1945, Congress passed the McCarran-Ferguson Act, which granted states the power to regulate most aspects of the insurance business. The McCarran-Ferguson Act states that "no act of Congress shall be construed to invalidate, impair, or supersede any law enacted by any state for the purpose of regulating the business of insurance, or which imposes a fee or tax upon such business, unless such Act specifically relates to the business of insurance" (15 USC 1012(b)).

State regulation of insurance producers is centered on the protection of the consumer and consists primarily of licensing and continuing education requirements for producers. A producer generally must obtain a license from each state in which it sells insurance and for each product sold. Each state in which a producer sells insurance has regulatory authority over the producer's activities in the state.

The GLB Act does include several provisions that are designed to keep states from (1) unfairly regulating a bank to prevent it from engaging in

iaries are found in the Board's Regulation H (12 CFR 208.71–77).

4. See SR-02-01, "Revisions to Bank Holding Company Supervision Procedures for Organizations with Total Consolidated Assets of $5 Billion or Less," and section 1000.1 for a discussion of the Federal Reserve's risk-focused examinations and the risk-focused supervision program for community banking organizations. See also SR-97-24 and SR-97-25.

authorized insurance activities or (2) otherwise discriminating against banks engaged in insurance activities. These provisions are complex and beyond the scope of this guidance. However, the GLB Act generally does not prohibit a state from requiring a bank or bank employee engaged in insurance sales, solicitation, or cross-marketing activities to be licensed within the state.

State insurance regulatory authorities do not conduct routine, periodic examinations of an insurance producer. A state examination of an insurance producer is generally conducted only on an ad hoc basis and is primarily based on the volume and severity of consumer complaints. The state examination may also be based in part on the producer's market share and on previous examination findings. Additionally, a review of a producer would typically not assess its financial condition.

A state's market conduct examination of *insurance sales practices* is focused at the insurance-underwriter level.[5] The insurance underwriter is generally held accountable for compliance with state insurance laws to protect the consumer from the unfair sales practices of any producer that markets the insurance underwriter's products. Market conduct examinations of an insurance underwriter may potentially uncover a concern about a particular producer, such as a bank-affiliated producer.[6] However, in the past, a state insurance regulatory authority has not typically examined a producer unless the producer is owned by the insurance underwriter.

Generally, market conduct examinations include reviews of the insurance underwriters' complaint handling, producer licensing, policyholder service, and marketing and sales practices. Typically, a state authority will direct a corrective action for insurance sales activity at the underwriter. The states generally have specific guidance for their market conduct examinations of life, health, and property/casualty[7] lines of business—guidance that corresponds to regulations related to advertising, misrepresentations, and disclosures for these different business lines. The reports of examination issued by the state insurance departments are usually available to the public.

Because the underwriter, not the producer, is liable to the insured, the failure of an insurance producer generally would not result in financial loss to consumers or state guarantee funds. Consequently, there are no regulatory capital requirements for insurance producers, nor do states require regulatory reporting of financial statement data on insurance producers. While the underwriter is ultimately liable to the insured, in some instances, a producer and its owner may be held liable for misrepresentations, as well as for violations of laws and regulations.

Functional Regulation

Under the GLB Act, banking supervisors' reviews of insurance or securities activities conducted in a bank's functionally regulated subsidiary are not to be extensions of more traditional bank-like supervision. Rather, to the extent possible, bank supervisors are to rely on the functional regulators to appropriately supervise the insurance and securities activities of a functionally regulated subsidiary. A functionally regulated subsidiary includes any subsidiary of a bank that (1) is engaged in insurance activities and subject to supervision by a state insurance regulator or (2) is registered as a broker-dealer with the Securities and Exchange Commission. The GLB Act does *not* limit the Federal Reserve's supervisory authority with respect to a *bank* or the insurance activities conducted by a bank. The functional regulators for insurance sales activities, including the activities of insurance producers, consist of the insurance departments in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, American Samoa, and Guam.

5. Generally, market conduct reviews of *insurance underwriters* are conducted on an ad hoc basis, triggered primarily by the volume and severity of consumer complaints, and are based on the underwriter's market share or on previous examination findings. In some states, however, market conduct reviews of insurance underwriters are conducted on a periodic, three- to five-year schedule.

6. The terms "insurance underwriter," "insurer," "insurance carrier," and "insurance company" are industry terms that apply similarly to the party to an insurance arrangement who undertakes to indemnify for losses, that is, the party that assumes the principal risk under the contract.

7. Property insurance indemnifies a person who has an interest in a physical property for loss of the property or the loss of its income-producing abilities. Casualty insurance is primarily concerned with the legal liability for losses caused by injury to persons or damage to the property of others. It may also include such diverse forms of insurance as crime insurance, boiler and machinery insurance, and aviation insurance. Many casualty insurers also underwrite surety bonds.

The GLB Act places certain limits on the ability of the Federal Reserve to examine, obtain reports from, or take enforcement action against a functionally regulated nondepository subsidiary of a state member bank. For purposes of these limitations, a subsidiary licensed by a state insurance department to conduct insurance sales activities is considered functionally regulated only with respect to its insurance activities and any activities incidental to these activities.[8]

The GLB Act indicates that the Federal Reserve must rely, to the fullest extent possible, on information obtained by the appropriate state insurance authority of a nondepository insurance agency subsidiary of a state member bank. In addition, the Federal Reserve may examine a functionally regulated subsidiary of a state member bank only in the following situations:

- The Federal Reserve has reasonable cause to believe that the subsidiary is engaged in activities that pose a material risk to an affiliated depository institution, as determined by the responsible Reserve Bank and Board staff.
- After reviewing relevant information (including information obtained from the appropriate functional regulator), it is determined that an examination is necessary to adequately understand and assess the banking organization's systems for monitoring and controlling the financial and operational risks that may pose a threat to the safety and soundness of an affiliated depository institution.
- On the basis of reports and other available information (including information obtained from the appropriate functional regulator), there is reasonable cause to believe that the subsidiary is not in compliance with a federal law that the Federal Reserve has specific jurisdiction to enforce with respect to the subsidiary (including limits relating to transactions with affiliated depository institutions), and the Federal Reserve cannot assess such compliance by examining the state member bank or other affiliated depository institution.

Other similar restrictions limit the ability of the Federal Reserve to obtain a report directly from, or take enforcement action against, a functionally regulated nonbank subsidiary of a state member bank. These GLB Act limitations do *not* apply to a state member bank even if the state member bank is itself licensed by a state insurance regulatory authority to conduct insurance sales activities.

Staff who are conducting reviews of state member bank insurance or annuity sales activities should be thoroughly familiar with SR-00-13, which provides guidance on reviews of functionally regulated state member bank subsidiaries. Reserve Bank staff may conduct an examination of a functionally regulated subsidiary, or request a specialized report from a functionally regulated subsidiary, only after obtaining approvals from the appropriate staff of the Board's Division of Banking Supervision and Regulation.

When preparing or updating the risk assessment of a state member bank's insurance or annuity sales activities, Federal Reserve staff, when appropriate, should coordinate their activities with the appropriate state insurance authorities. The Federal Reserve's supervision of state member banks engaged in insurance sales activities is not intended to replace or duplicate the regulation of insurance activities by the appropriate state insurance authorities.

Information Sharing with the Functional Regulator

The Federal Reserve and the National Association of Insurance Commissioners (NAIC) approved a model memorandum of understanding (MOU) on the sharing of confidential information between the Federal Reserve and individual state insurance departments.[9] The Board also approved the delegation of authority to the Board's general counsel to execute agreements with individual states, based on this MOU. Examiners should follow required Board administrative procedures before sharing any confidential information with a state insurance regulator. (These procedures generally require Federal Reserve staff to identify and forward to Board staff for review any confidential information that may be appropriate to share with the applicable

8. For example, if a state member bank subsidiary engages in mortgage lending and is also licensed as an insurance agency, it would be considered a functionally regulated subsidiary only to the extent of its insurance sales activities.

9. The NAIC is the organization of insurance regulators from the 50 states, the District of Columbia, and the four U. S. territories. The NAIC provides a forum for the development of uniform policy among the states and territories. The NAIC is not a governmental or regulatory body.

state insurance regulator concerning insurance sales activities conducted by state member banks.) The Board's Division of Consumer and Community Affairs CP Letter 2001-11 outlines the procedures for sharing consumer complaint information with state insurance regulators.

STATUTORY AND REGULATORY REQUIREMENTS AND POLICY GUIDANCE

Privacy Rule and the Fair Credit Reporting Act

State member banks that sell insurance to consumers must comply with the privacy provisions under title V of the GLB Act (12 USC 6801–6809), as implemented by the Board's Regulation P (12 CFR 216) (the privacy rule). Functionally regulated state member bank nonbank insurance agency subsidiaries are not covered by the Federal Reserve's privacy rule; however, they must comply with the privacy regulations (if any) issued by their relevant state insurance regulator.

The privacy rule regulates a state member bank's treatment of nonpublic personal information about a "consumer," an individual who obtains a financial product or service (such as insurance) from the institution for personal, family, or household purposes. The privacy rule generally requires a bank to provide a notice to each of its customers that describes its privacy policies and practices no later than when the bank establishes a business relationship with the customer. The privacy rule also generally prohibits a bank from disclosing any nonpublic personal information about a consumer to any nonaffiliated third party, unless the bank first provides to the consumer a privacy notice and a reasonable opportunity to prevent (or "opt out" of) the disclosure, and the consumer does not opt out. The privacy rule permits a financial institution to provide a joint notice with one or more of its affiliates or other financial institutions, as identified in the privacy notice itself, provided that the notice is accurate with respect to the institution and the other institutions.

While the privacy rule applies to the sharing of nonpublic personal information by a bank with nonaffiliated third parties, the sharing of certain consumer information with affiliates or nonaffiliates may be subject to the Fair Credit Reporting Act (FCRA) as well. For example, under the FCRA, if a bank wants to share with its insurance subsidiary information from a credit report or from a consumer application for credit (such as the consumer's assets, income, or marital status), the bank must first notify the consumer about the intended sharing and give the consumer an opportunity to opt out. The same rules would apply to an insurance company that wants to share information from credit reports or from applications for insurance with an affiliate or a third party.

Anti-Tying Prohibitions

Federal law (section 106(b) of the BHC Act Amendments of 1970 (12 USC 1972(b))) generally prohibits a bank from requiring that a customer purchase a product or service from the bank or an affiliate as a prerequisite to obtaining another product or service (or a discount on the other product or service) from the bank. This prohibition applies whether the customer is retail or institutional, or whether the transaction is on bank premises or off premises. For example, a state member bank may not require that a customer purchase insurance from the bank or a subsidiary or affiliate of the bank in order to obtain a loan from the bank (or a reduced interest rate on the loan).[10]

Policy Statement on Income from Sale of Credit Life Insurance

The Federal Reserve Board's Policy Statement on Income from Sale of Credit Life Insurance (see the *Federal Reserve Regulatory Service* at 3-1556) sets forth the principles and standards that apply to a bank's sales of credit life insurance and the limitations that apply to the receipt of income from those sales by certain individuals and entities associated with the bank. See also the examination procedures related to this policy statement in section 2130.3.

10. See section 2040.1 and "Tie-In Considerations of the BHC Act," section 3500.0, of the *Bank Holding Company Supervision Manual.*

RISK-MANAGEMENT PROGRAM

Elements of a Sound Insurance or Annuity Sales Program

A state member bank engaged in insurance or annuity sales activities should—

- conduct insurance sales programs in a safe and sound manner;
- have appropriate written policies and procedures in place that are commensurate with the volume and complexity of its insurance sales activities;
- obtain its board of directors' approval of the scope of the insurance and annuity sales program and of written policies and procedures for the program;
- effectively oversee the sales program activities, including third-party arrangements;
- have an effective, independent internal audit and compliance program;
- appropriately train and supervise the employees conducting insurance and annuity sales activities;
- take reasonable precautions to ensure that disclosures to customers for insurance and annuity sales and solicitations are complete and accurate and are in compliance with applicable laws and regulations;
- ensure compliance with all applicable federal, state, or other jurisdiction regulations, including compliance with sections 23A and 23B of the Federal Reserve Act as that act applies to affiliate transactions; and
- have controls in place to ensure accurate and timely financial reporting.

Every state member bank conducting insurance or annuity sales activities should have appropriate, board-approved policies, procedures, and controls in place to monitor and ensure that it complies with both federal and state regulatory requirements. Consistent with the principle of functional regulation, the Federal Reserve will rely primarily on the appropriate state insurance authorities to monitor and enforce compliance with applicable state insurance laws and regulations, including state consumer protection laws and regulations governing insurance sales.

Sales Practices and Handling of Customer Complaints

Every state member bank engaged in insurance or annuity sales activities should have board-approved policies and procedures for handling customer complaints related to these sales. The customer complaint process should provide for the recording and tracking of all complaints and require periodic reviews of complaints by compliance personnel. A state member bank's board of directors and senior management should also review complaints if the complaints involve significant compliance issues that may pose a risk to the state member bank.

Third-Party Arrangements

State member banks, to the extent permitted by applicable law, may enter into agreements with third parties, including unaffiliated agents or agencies, to sell insurance or annuities or provide expertise and services that otherwise would have to be developed in-house. Many banks hire third parties to assist in establishing an insurance program or to train their own insurance staff. A bank may also find it advantageous to offer more specialized insurance products through a third-party arrangement.

A state member bank's management should conduct a comprehensive review of an unaffiliated third party before entering into any arrangement to conduct insurance or annuity sales with the third party. The review should include an assessment of the third party's financial condition, management experience, reputation, and ability to fulfill its contractual obligations to the state member bank, which includes compliance with applicable consumer protection laws and regulations.

The state member bank's board of directors or its designated committee should approve any agreements with third parties. Agreements should outline the duties and responsibilities of each party; describe the third-party activities permitted on the institution's premises; address the sharing or use of confidential customer information; and define the terms for use of the state member bank's office space, equipment, and personnel. If an arrangement includes dual employees (for example, bank employees who are also employed by an independent third party), the agreement must provide for written employment contracts that specify the duties of

these employees and their compensation arrangements.

In addition, a third-party agreement should specify that the third party will comply with all applicable laws and regulations and will conduct its activities in a manner consistent with the CPSI regulation, if applicable. The agreement should authorize the banking organization to monitor the third party's compliance with its agreement, as well as authorize the bank to have access to third-party records considered necessary to evaluate compliance. A state member bank that contracts with a functionally regulated third party should obtain from and review, as appropriate, any relevant, publicly available regulatory reports of examination of the third party.[11] Finally, the agreement should provide for indemnification of the institution by the unaffiliated third party for any losses caused by the conduct of the third party's employees in connection with its sales activities.

The state member bank is responsible for ensuring that any third party or dual employee selling insurance at or on behalf of the bank is appropriately trained either by the bank or the third party with respect to compliance with the minimum disclosures and other requirements of the CPSI regulation and applicable state regulations. The banking organization should obtain and review copies of third-party training and compliance materials to monitor the third party's performance of its disclosure and training obligations.

Designation, Training, and Supervision of Personnel

A state member bank hiring personnel to sell insurance or annuities should investigate the backgrounds of the prospective employees. When a candidate for employment has previous insurance industry experience, the state member bank should have procedures to determine whether the individual has been the subject of any disciplinary actions by state insurance regulators.[12]

The state member bank should require its own insurance or annuity sales personnel or third-party sales personnel selling at or on behalf of the bank to receive appropriate training and licensing. Training should cover appropriate policies and procedures for the bank's sales of insurance and annuity products. Personnel who are referring potential or established customers to a licensed insurance producer should also be trained to ensure that referrals are made in conformance with the CPSI regulation, if applicable. The training should also include procedures and guidance to ensure that an unlicensed or referring individual cannot be deemed to be acting as an insurance agent that is subject to licensing requirements.

When insurance or annuities are sold by a state member bank or third parties at an office of, or on behalf of, the organization, the institution should have policies and procedures to designate, by title or name, the individuals responsible for supervising insurance sales activities, as well as for supervising the referral activities of bank employees not authorized to sell these products. A state member bank also should designate supervisory personnel responsible for monitoring compliance with any third-party agreement, as well as with the CPSI regulation, if applicable.

Compliance

State member banks should have policies and procedures to ensure that insurance or annuity sales activities are conducted in compliance with applicable laws and regulations (including the CPSI regulation for sales conducted by or on behalf of the state member bank) and the institution's internal policies and procedures. Compliance procedures should identify any potential conflicts of interest and how such conflicts should be addressed. For example, sales-compensation programs should be conducted in a manner that would not expose the bank to undue legal or reputation risks. The compliance procedures should also provide for a system to monitor customer complaints and their resolution. Where applicable, compliance procedures also should call for verification that third-party sales are being conducted in a manner consistent with the governing agreement with the banking organization.

The compliance function should be conducted independently of the insurance and annuity prod-

11. The reports of examination issued by state insurance regulators are generally public documents. Many states do not conduct periodic examinations of insurance sales activities.

12. Information from the states on the issuance and termination of producer licenses and on producers' compliance with continuing education requirements is available from the NAIC database known as the National Insurance Producer Registry (NIPR).

uct sales and management activities. Compliance personnel should determine the scope and frequency of their reviews, and findings of compliance reviews should be reported directly to the state member bank's board of directors or to its designated board committee.

RISK ASSESSMENT OF INSURANCE AND ANNUITY SALES ACTIVITIES

A risk assessment of insurance activities may be accomplished in the course of conducting a regularly scheduled state member bank examination or as a targeted review. The purpose of preparing the risk assessment is to determine the level and direction of risk to the bank arising from its insurance and annuity sales activities. Risks to state member banks engaged in insurance and annuity sales programs consist primarily of legal, reputational, and operational risk, all of which may lead to financial loss. After completing the risk assessment, if material concerns remain, the Board's Division of Banking Supervision and Regulation staff should be consulted for further guidance.

Legal and reputational risk may arise from a variety of sources, such as fraud; noncompliance with statutory or regulatory requirements, including those pertaining to the handling of premiums collected on behalf of the underwriter; claims processing; insurance and annuity sales practices; and the handling of ''errors and omissions'' claims.[13] Other sources of legal and reputational risk may arise from failing to safeguard nonpublic customer information, a high volume of customer complaints, or public regulatory sanctions against a producer.

Legal and reputational risks may also arise from an agent's obligation to provide a customer with products that are suited to the customer's particular needs and are priced and sold in accordance with state regulations. Additionally, an agent or agency may be liable for failing to carry out the appropriate paperwork to bind a policy that it has sold to a customer, or for making an error in binding the policy. State insurance departments generally are permitted by law to suspend or revoke a producer's license and assess monetary penalties against a producer if warranted.

Operational risk may arise from errors in processing sales-related information or from a lack of appropriate controls over systems or staff responsible for carrying out the insurance or annuity sales activities. Additionally, state member banks that have recently commenced insurance or annuity sales activities, or that are expanding their insurance or annuity sales business, also are exposed to risk arising from inadequate strategic and financial planning associated with the activities, which could result in financial loss. Examiners should be attuned to risks that may arise from inadequate controls over insurance activities, a rapid expansion of the insurance or annuity sales programs offered by the state member bank, the introduction of new products or delivery channels, and legal and regulatory developments.

Operational risk may arise from inadequate premium-payment procedures and trust-account-balance administration by an agency. When the insurance agency bills the insured, the agent must comply with requirements for forwarding the payments to the insurer and for safekeeping the funds. Inadequate internal controls over this activity may result in the inappropriate use of these funds by the agent or agency. The state member bank should ensure that appropriate controls are in place to verify that all funds that are owed to the insurer or the insured are identified in the trust account and that the account is in balance.

When conducting a risk assessment, the examiner should first obtain relevant information to determine the existence and scale of insurance or annuity sales activity. Such information is available in the state member bank's Uniform Bank Performance Report (UBPR) and in other System reports on insurance activities. Relevant reports, including applicable balance sheets and income statements for the insurance and annuity sales activities, may also be obtained from the state member bank. When preparing a risk assessment for an insurance or annuity sales activity that is conducted by a functionally regulated nonbank subsidiary of a state member bank, examiners should rely, to the fullest extent possible, on information available from the state member bank and the appropriate state insurance regulator for the subsidiary. If information that is needed to assess the risk cannot be obtained from the state member bank or the

13. Errors and omissions insurance indemnifies the insured against loss sustained because of an error or oversight by the insured. For instance, an insurance agency generally purchases this type of coverage to protect itself against such things as failing to issue a policy.

applicable functional regulator, the examiner should consult with the appropriate designated Board staff. Requests should not be made directly to a functionally regulated nonbank insurance and annuity sales subsidiary of a state member bank without first obtaining approval from the appropriate Board staff.

CONSUMER PROTECTION IN SALES OF INSURANCE RULES

Overview of the CPSI Regulation

The CPSI regulation is applicable to all insured depository institutions.[14] The regulation, however, generally does not apply to nonbank affiliates or subsidiaries of a state member bank unless the company engages in the retail sale of insurance products or annuities at an office of, or on behalf of, an insured depository institution. Interpretations of the regulation issued by the federal banking agencies are found in appendix A of this section. Federal Reserve examiners are responsible for reviewing state member banks' compliance with the regulation.

The regulation applies to the retail sale of insurance products and annuities by banks or by any other person at an office of a bank, or acting on behalf of a bank. For purposes of the CPSI regulation, ''office'' means the premises of the bank where retail deposits are accepted. The regulation applies only to the retail sale of insurance or annuity products—that is, when the insurance is sold or marketed to an individual primarily for personal, family, or household purposes.

Misrepresentations Prohibited

The regulation prohibits a bank or other covered person from engaging in any practice or using any advertisement at any office of, or on behalf of, the bank or a subsidiary of the bank if the practice or advertisement could mislead any person or otherwise cause a reasonable person to erroneously believe—

- that the insurance product or annuity is backed by the federal government or the bank or is insured by the Federal Deposit Insurance Corporation (FDIC);
- that an insurance product or annuity does not have investment risk, including the potential that principal may be lost and the product may decline in value, when in fact the product or annuity does have such risks; or
- in the case of a bank or subsidiary of the bank at which insurance products or annuities are sold or offered for sale, that (1) the bank may condition approval of an extension of credit to a consumer by the bank or subsidiary on the purchase of an insurance product or annuity from the bank or a subsidiary of the bank, and (2) the consumer is not free to purchase the insurance product or annuity from another source.

The regulation also incorporates the anti-tying provisions of section 106(b) of the Bank Holding Company Act Amendments of 1970 (12 USC 1972). Additionally, banks are prohibited from selling life or health insurance products if the status of the applicant or insured as a victim of domestic violence or as a provider of services to domestic violence victims is considered as a factor in decision making on the product, except as expressly authorized by state law.

Insurance Disclosures

The CPSI regulation also requires that a bank or a person selling insurance at an office of, or on behalf of, a bank make the following affirmative disclosures (to the extent accurate), both orally and in writing, before the completion of the initial sale of an insurance product or an annuity to a consumer. However, sales by mail or, if the consumer consents, via electronic media (such as the Internet) do not require oral disclosure.

- The insurance product or annuity is not a deposit or other obligation of, or guaranteed by, the bank or an affiliate of the bank.
- The insurance product or annuity is not insured by the FDIC or any other U.S. government agency, the bank, or (if applicable) an affiliate of the bank.
- The insurance product or annuity, if applicable, has investment risk, including the possible loss of value.

14. The CPSI regulation applies to all federally insured depository institutions, including all federally chartered U.S. branches and state-chartered insured U.S. branches of foreign banking organizations.

For telephone sales, written disclosures must be mailed within three business days. The above disclosures must be included in advertisements and promotional materials for insurance products and annuities, unless the advertisements or promotional materials are of a general nature and describe or list the nature of services or products offered by the bank. Disclosures must be conspicuous and readily understandable.

Credit Disclosures

When an application for credit is made in connection with the solicitation, offer, or sale of an insurance product or annuity, the consumer must be notified that the bank may not condition the extension of credit on either (1) the consumer's purchase of an insurance product or annuity from the bank or any of its affiliates or (2) the consumer's agreement not to obtain, or a prohibition on the consumer from obtaining, an insurance product or annuity from an unaffiliated entity. These disclosures must be made both orally and in writing; however, applications taken by mail or, if the consumer consents, via electronic media, do not require oral disclosure. For telephone applications, the written disclosure must be mailed within three business days. The disclosures must be conspicuous and readily understandable.

Consumer Acknowledgment

The bank must obtain written or electronic acknowledgments of the consumer's receipt of the disclosures described above at the time they are made or at the completion of the initial purchase. For telephone sales, the bank must receive an oral acknowledgment and make a reasonable effort to obtain a subsequent written or electronic acknowledgment.

Location

Insurance and annuity sales activities must take place, to the extent practicable, in an area physically segregated from one where retail deposits are routinely accepted from the general public (such as teller windows). The bank must clearly identify and delineate areas where insurance and annuity sales activities occur.

Referrals

Any person who accepts deposits from the public in an area where deposits are routinely accepted may refer a consumer to a qualified person who sells insurance products or annuities only if the person making the referral receives no more than a one-time, nominal fee of a fixed dollar amount for the referral. The amount of the referral fee may *not* depend on whether a sale results from the referral.

Qualifications

A bank may not permit any person to sell or offer insurance products or annuities at its office or on its behalf, unless that person is at all times properly qualified and licensed under applicable state law for the specific products being sold or recommended.

Relationship of the CPSI Regulation to State Regulation

The GLB Act contains a legal framework for determining the effect of the CPSI regulation on state laws governing the sale of insurance, including state consumer protection standards. In general, if a state has legal requirements that are inconsistent with, or contrary to, the CPSI regulation, initially the federal regulation does not apply in the state. However, the federal banking agencies may, after consulting with the state involved, decide to preempt any inconsistent or contrary state laws if the agencies find that the CPSI regulation provides greater protections than the state laws. It is not expected that there will be significant conflict between state and federal laws in this area. If the consumer protection laws of a particular state appear to be inconsistent with and less stringent (that is, provide less consumer protection) than the CPSI regulation, examiners should inform the staff of the Board's Division of Banking Supervision and Regulation.

Relationship to Federal Reserve Guidance on the Sale of Nondeposit Investment Products

When a bank sells insurance products or annu-

ities that also are securities (such as variable life insurance annuities), it must conform with the applicable Federal Reserve and interagency guidance pertaining to a bank's retail sales of nondeposit investment products (NDIPs).[15] If the CPSI regulation and the guidance pertaining to NDIPs conflict, the CPSI regulation prevails.

Examining a State Member Bank for Compliance with the CPSI Regulation

Examinations for compliance with the CPSI regulation should be conducted consistent with the risk-focused supervisory approach when a state member bank sells insurance products or annuities directly, or when a third party sells insurance or annuities at or on behalf of, a state member bank. To the extent practicable, the examiner should conduct the review at the state member bank. In certain instances, however, the examiner's review at the state member bank may identify potential supervisory concerns about the state member bank's compliance with the CPSI regulation as it pertains to insurance or annuities sales conducted by a functionally regulated nonbank affiliate or subsidiary of the state member bank that is selling insurance products or annuities at or on behalf of the state member bank.

If the examiner determines that an on-site review of a functionally regulated nonbank affiliate or subsidiary of the state member bank is appropriate to adequately assess the state member bank's compliance with the CPSI regulation, the examiner should discuss the situation with staff of the Board's Division of Banking Supervision and Regulation. The approval of the Division of Banking Supervision and Regulation's officer that is responsible for the supervisory policy and examination guidance pertaining to insurance and annuity sales activities should be obtained before examining or requesting any information directly from a functionally regulated nonbank affiliate or subsidiary of the state member bank that is selling insurance or annuity products at or on behalf of the state member bank.

The examination guidelines described in section 4043.3 apply to retail sales, solicitations, advertisements, or offers of insurance products and annuities by any state member bank or any other person that is engaged in such activities at an office of the bank or on behalf of the state member bank. For purposes of the CPSI regulation, activities "on behalf of a state member bank" include activities in which a person, whether at an office of the bank or at another location, sells, solicits, advertises, or offers an insurance product or annuity and in which at least one of the following applies:

- The person represents to a consumer that the sale, solicitation, advertisement, or offer of any insurance product or annuity is by or on behalf of the bank.
- The bank refers a consumer to a seller of insurance products or annuities, and the bank has a contractual arrangement to receive commissions or fees derived from the sale of an insurance product or annuity resulting from the bank's referral.
- Documents evidencing the sale, solicitation, advertising, or offer of an insurance product or annuity identify or refer to the bank.

APPENDIX A—JOINT INTERPRETATIONS OF THE CONSUMER PROTECTION IN SALES OF INSURANCE REGULATION

In response to a banking association's inquiries, the federal banking agencies jointly issued interpretations regarding the Consumer Protection in Sales of Insurance (CPSI) regulation.[1] A joint statement, issued on August 17, 2001, contains responses to a set of questions relating to disclosure and acknowledgment, the scope of applicability of the regulation, and compliance. Additionally, a February 28, 2003, joint statement responded to a request to clarify whether the disclosure requirements apply to renewals of pre-existing insurance policies sold before October 1, 2001, the effective date of the regulation. The issues raised and the banking agencies' responses are summarized below.

15. Interagency Statement on Retail Sales of Nondeposit Investment Products, February 17, 1994. See SR-94-11.

1. These letters, issued jointly by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision, may be accessed on these agencies' web sites.

Disclosures

Credit Disclosures

A bank or other person who engages in insurance sales activities at an office of, or on behalf of, a bank (“a covered person”) must make the credit disclosures set forth in the regulation if a consumer is solicited to purchase insurance while the consumer’s loan application is pending. A consumer’s application for credit is still “pending” for purposes of the regulation if the depository institution has approved the consumer’s loan application but not yet notified the consumer. Until the consumer is notified of the loan approval, the covered person must provide the credit disclosures if the consumer is solicited, offered, or sold insurance.

Disclosures for Sales by Mail and Telephone

The regulation requires a covered person to provide oral disclosures and to obtain an oral acknowledgment of these disclosures when sales activities are conducted by telephone. This requirement applies regardless of whether the consumer will also receive and acknowledge written disclosures in person, through the mail, or electronically.

Use of Short-Form Insurance Disclosures

There is no short form for the credit disclosures. A depository institution, however, may use the short-form insurance disclosures set forth below in visual media (such as television broadcasting, ATM screens, billboards, signs, posters, and written advertisements and promotional materials):

- NOT A DEPOSIT
- NOT FDIC-INSURED
- NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY
- NOT GUARANTEED BY THE BANK
- MAY GO DOWN IN VALUE

Acknowledgment of Disclosures

Reasonable efforts to obtain written acknowledgment. The banking agencies have not prescribed any steps that must be taken for a depository institution’s efforts to obtain a written acknowledgment to be deemed “reasonable” in a transaction conducted by telephone. Examples of reasonable efforts, however, include—

- providing the consumer with a return-addressed envelope or similar means to facilitate the consumer’s return of the written acknowledgment,
- making a follow-up phone call or contact,
- sending a second mailing, or
- similar actions.

The covered person should (1) maintain documentation that the written disclosures and the request for written acknowledgment of those disclosures were mailed to the consumer and (2) should record his or her efforts to obtain the signed acknowledgment. The “reasonable efforts” policy exception for telephone sales does not apply to other types of transactions, such as mail solicitations, in which a covered person must obtain from the consumer a written (in electronic or paper form) acknowledgment.

Appropriate form or format for acknowledgment provided electronically. Electronic acknowledgments are not required to be in a specific format but must be consistent with the provisions of the CPSI regulation applicable to consumer acknowledgments. That is, the electronic acknowledgment must establish that the consumer has acknowledged receipt of the credit and insurance disclosures, as applicable.

Retention of acknowledgments by an insurance company. If an insurance company provides the disclosures and obtains the acknowledgment on behalf of a depository institution, the insurance company may retain the acknowledgment. The depository institution is responsible for ensuring that sales made “on behalf of” the depository institution are in compliance with the CPSI regulation. An insurance company may maintain documentation showing compliance with the CPSI regulation, but the depository institution should have access to such records and the records should be readily available for review by examiners.

Form of written acknowledgment. There is no prescribed form for the written acknowledg-

ment. The regulation requires, however, that a covered person obtain the consumer's acknowledgment of receipt of the complete insurance and credit disclosures.

Timing of acknowledgment receipt. A covered person must obtain the consumer's acknowledgment either at the time a consumer receives disclosures or at the time of the initial purchase of an insurance product.

Oral acknowledgment of oral disclosure. The CPSI regulation does not prescribe any specific wording for an oral acknowledgment. However, if a covered person has made the insurance and credit disclosures orally, an affirmative response to the question "Do you acknowledge that you received this disclosure?" is acceptable.

Scope of the CPSI Regulation

Applicability to Private Mortgage Insurance

Depending on the nature of a depository institution's involvement in an insurance sales transaction, the CPSI regulation may cover sales of private mortgage insurance. If the depository institution itself purchases the insurance to protect its interest in mortgage loans it has issued and merely passes the costs of the insurance on to the mortgage borrowers, the transaction is not covered by the regulation. If, however, a consumer has the option of purchasing the private mortgage insurance and (1) the depository institution offers the private mortgage insurance to a consumer or (2) any other person offers the private mortgage insurance to a consumer at an office of a depository institution, or on behalf of a depository institution, the transaction would be covered by the regulation.

Applicability to Federal Crop Insurance

The CPSI regulation does not apply to federal crop insurance that is sold for commercial or business purposes. However, if the crop insurance is purchased by an individual primarily for family, personal, or household purposes, it would be covered.

Solicitations and Applications Distributed Before, but Returned After, the Effective Date of the CPSI Regulation

Direct-mail solicitations and "take-one" applications that are distributed on or after October 1, 2001, must comply with the CPSI regulation. If a consumer seeks to purchase insurance after the effective date of the regulation in response to a solicitation or advertisement that was distributed *before* that date, the depository institution would be in compliance with the regulation if the institution provides the consumer, before the initial sale, with the disclosures required by the regulation. These disclosures must be both written and oral, except that oral disclosures are not required if the consumer mails in the application.

Renewals of Insurance

Renewals of insurance are not subject to the disclosure requirements (see "Disclosures" above) but are subject to other requirements of the CPSI regulation. A "renewal" of insurance means continuation of coverage involving the same type of insurance for a consumer as issued by the same carrier. A renewal need not be on the same terms and conditions as the original policy, provided that the renewal does not involve a different type of insurance and the consumer has previously received the disclosures required by the regulation at the time of the initial sale. An upgrade in coverage at a time when a policy is not up for renewal would be treated as a renewal, provided that the solicitation and sale of the upgrade does not involve a different type of insurance and the consumer has previously received the disclosures required by the regulation at the initial sale.

Disclosures Required with Renewals of Insurance Coverage

The banking agencies' interpretations clarified that the CPSI regulation does not *mandate* disclosures for renewals of policies sold before October 1, 2001. Accordingly, the regulation does not require the disclosures to be furnished at the time of renewal of a policy, including a pre-existing policy. However, renewals are subject to the other provisions of the regulation. Moreover, the banking agencies would expect that, consistent with applicable safety-and-

soundness requirements, depository institutions would take reasonable steps to avoid customer confusion in connection with renewals of pre-existing policies.

"On-Behalf-of" Test and Use of Corporate Name or Logo

Under the CPSI regulation, an affiliate of a bank is not considered to be acting "on behalf of" a bank simply because the affiliate's marketing or other materials use a corporate name or logo that is common to the bank and the affiliate. In general, this exclusion applies even if a bank and its parent holding company have a similar, but not identical, name. For example, if the names of all of the affiliates of a bank holding company share the words "First National," an affiliate would not be considered to be engaged in an activity "on behalf of" an affiliated bank simply by using the terms "First National" as part of a corporate logo or identity. The affiliate would, however, be considered to be acting "on behalf of" an affiliated bank if the name of the bank (for example, "First National Bank") appears in a document as the seller, solicitor, advertiser, or offeror of insurance. A transaction also would be covered if it occurs on the premises of a depository institution or if one of the other prongs of the "on-behalf-of" test is met.

Compliance

Appropriate Documentation of an Oral Disclosure or Oral Acknowledgment

There is no specific documentation requirement for oral disclosures or acknowledgments. However, other applicable regulatory reporting standards would apply. Appropriate documentation of an oral disclosure would clearly show that the covered person made the credit and insurance disclosures to a consumer. Similarly, appropriate documentation of an oral acknowledgment would clearly show that the consumer acknowledged receiving the credit and insurance disclosures. For example, a tape recording of the conversation (where permitted by applicable laws) in which the covered person made the oral disclosures and received the oral acknowledgment would be acceptable. Another example would be a contemporaneous checklist completed by the covered person to indicate that he or she made the oral disclosures and received the oral acknowledgment. A contemporaneous note to the consumer's file would also be adequate. The documentation should be maintained in the consumer's file so that it is accessible to examiners.

Setting for Insurance Sales

A depository institution must identify the areas where insurance sales occur and must clearly delineate and distinguish those areas from areas where the depository institution's retail deposit-taking activities occur. Although the banking agencies did not define how depository institutions could "clearly delineate and distinguish" insurance areas, signage or other means may be used.

APPENDIX B—GLOSSARY

For additional definitions of insurance terms, see section 4040.1.

Accident and health insurance. A type of coverage that pays benefits in case of sickness, accidental injury, or accidental death. This coverage may provide for loss of income when the insured is disabled and provides reimbursement for medical expenses when the insured is ill. The insurance can provide for debt payment if it is taken out in conjunction with a loan. (See *Credit life insurance.*)

Actuary. A professional whose function is to calculate statistically various estimates for the field of insurance, including the estimated risk of loss on an insurable interest and the appropriate level for premiums and reserves.

Admitted insurer. An insurance company licensed by a state insurance department to underwrite insurance products in that state.

Agency contract (or agreement). An agreement that establishes the contractual relationship between an agent and an insurer.

Agent. A licensed insurance company representative under contract to one or more insurance companies. Depending on the line of insurance

represented, an agent's power may include soliciting, advertising, and selling insurance; collecting premiums; claims processing; and effecting insurance coverage on behalf of an insurance underwriter. Agents are generally compensated by commissions on policies sold, although some may receive salaries.

- *Captive or exclusive agent.* An agent who represents a single insurer.

- *General agent.* An agent who is contractually awarded a specific geographic territory for an individual insurance company. They are responsible for building their own agency and usually represent only one insurer. Unlike exclusive agents, who usually receive a salary in addition to commissions, general agents are typically compensated on a commission basis only.

- *Independent agent.* An agent who is under contractual agreements with at least two different insurers. Typically, all of the independent agent's compensation originates from commissions.

Aggregate excess-of-loss reinsurance. A form of "excess-of-loss" reinsurance that indemnifies the ceding company against the amount by which all of the ceding company's losses incurred during a specific period (usually 12 months) exceed either (1) a predetermined dollar amount or (2) a percentage of the company's subject premiums. This type of contract is also commonly referred to as *stop-loss reinsurance* or *excess-of-loss ratio reinsurance.*

Allied lines. Various insurance coverages for additional types of losses and against losses by additional perils. The coverages are closely associated with and usually sold with fire insurance. Examples include coverage against loss by perils other than fire, coverage for sprinkler-leakage damage, and business-interruption coverage.

Annuity. A contract that provides for a series of payments payable over an individual's life span or other term, on the basis of an initial lump-sum contribution or series of payments made by the annuitant into the annuity during the accumulation phase of the contract.

- *Fixed-annuity contracts* provide for payments to annuitants at fixed, guaranteed minimum rates of interests.

- *Variable-annuity contracts* provide for payments based on the performance of annuity investments. Variable-annuity contracts are usually sold based on a series of payments and offer a range of investment or funding options, such as stocks, bonds, and money market fund investments. The annuity principal and the investment return are not guaranteed as they depend on the performance of the underlying funding option.

Annuity payments may commence with the execution of the annuity contract (*immediate annuity*) or may be deferred until some future date (*deferred annuity*).

Assigned risk. A risk that is not usually acceptable to insurers and is therefore assigned to a group of insurers who are required to share in the premium income and losses, in accordance with state requirements, in order for the insurer to sell insurance in the state.

Assignment. The legal transfer of one person's interest in an insurance policy to another person or business.

Bank-owned life insurance (BOLI). Life insurance purchased and owned by a bank to fund its exposure arising from employee compensation and benefit programs. In a typical BOLI program, a bank insures a group of employees; pays the life insurance policy premiums; owns the cash values of the policies, which are booked on the bank's balance sheet as "other assets"; and is the beneficiary of the policies upon the death of any insured employee or former employee. (See SR-04-19 and section 4042.1.)

Beneficiary. The person or entity named in an insurance policy as the recipient of insurance proceeds upon the policyholder's death or when an endorsement matures. A revocable beneficiary can be changed by the policyholder at any time. An irrevocable beneficiary can be changed by the policyholder only with the written permission of the beneficiary.

Binder. A written or oral agreement, typically issued by an insurer, agent, or broker for property and casualty insurance, to indicate acceptance of a person's application for insurance and

to provide interim coverage pending the insurance company's issuance of a binding policy.

Blanket bond. Coverage for an employer for loss incurred as a result of employee dishonesty.

Boiler and machinery insurance. Insurance against the sudden and accidental breakdown of boilers, machinery, and electrical equipment, including coverage for damage to the equipment and property damage, including the property of others. Coverage can be extended to cover consequential losses, including loss from interruption of business.

Broker. A person who represents the insurance buyer in the purchase of insurance. Brokers do not have the power to bind an insurance company to an insurance contract. Once a contract is accepted, the broker is compensated for the transaction through a commission from the insurance company. An individual may be licensed as both a broker and an agent.

Bulk reinsurance. A transaction sometimes defined by statute as any quota-share, surplus aid, or portfolio reinsurance agreement through which an insurer assumes all or a substantial portion of the liability of the reinsured company.

Captive insurer. An insurance company established by a parent firm to insure or reinsure its own risks or the risks of affiliated companies. A captive may also underwrite insurable risks of unaffiliated companies, typically the risks of its customers or employees. A captive insurer may underwrite credit life or private mortgage insurance (third-party risks) related to its lending activities.

Cash surrender value of life insurance. The amount of cash available to a life insurance policyholder upon the voluntary termination of a life insurance policy before it becomes payable by death or maturity.

Casualty insurance. Coverage for the liability arising from third-party claims against the insured for negligent acts or omissions causing bodily injury or property damage.

Cede. To transfer to a reinsurer all or part of the insurance or reinsurance risk underwritten by an insurance company.

Ceding commission. The fee paid to a reinsurance company for assuming the risk of a primary insurance company.

Ceding company (also cedant, reinsured, reassured). The insurer that transfers all or part of the insurance or reinsurance risk it has underwritten to another insurer or reinsurer via a reinsurance agreement.

Cession. The amount of insurance risk transferred to the reinsurer by the ceding company.

Churning. The illegal practice wherein a customer is persuaded to unnecessarily cancel one insurance policy in favor of buying a purportedly superior policy, often using the cash surrender value of the existing policy to pay the early premiums of the new policy. In such a transaction, the salesperson benefits from the additional commission awarded for booking a new policy.

Claim. A request for payment of a loss under the terms of a policy. Claims are payable in the manner suited to the insured risk. Life, property, casualty, health, and liability claims generally are paid in a lump sum after the loss is incurred. Disability and loss-of-time claims are paid periodically during the period of disability or through a discounted lump-sum payment.

Coinsurance. A provision in property and casualty insurance that requires the insured to maintain a specified amount of insurance based on the value of the property insured. Coinsurance clauses are also found in health insurance and require the insured to share a percentage of the loss.

Combination-plan reinsurance. A reinsurance agreement that combines the excess-of-loss and the quota-share forms of coverage within one contract, with the reinsurance premium established as a fixed percentage of the ceding company's subject premium. After deducting the excess recovery on any one loss for one risk, the reinsurer indemnifies the ceding company on the basis of a fixed quota-share percentage. If a loss does not exceed the excess-of-loss retention level, only the quota-share coverage applies.

Commission. The remuneration paid by insurance carriers to insurance agents and brokers for the sale of insurance and annuity products.

Comprehensive personal liability insurance. A type of insurance that reimburses the policyholder if he or she becomes liable to pay money for damage or injury he or she has caused to others. This coverage does not include automobile liability but does include almost every activity of the policyholder, except business operations.

Contractholder. The person, entity, or group to whom an annuity is issued.

Credit for reinsurance. A statutory accounting procedure, set forth under state insurance regulations, that permits a ceding company to treat amounts due from reinsurers as assets, or as offsets to liabilities, on the basis of the reinsurer's status.

Credit life insurance. A term insurance product issued on the life of a debtor that is tied to repayment of a specific loan or indebtedness. Proceeds of a credit life insurance policy are used to extinguish remaining indebtedness at the time of the borrower's death. The term is applied broadly to other forms of credit-related insurance that provide for debt satisfaction in the event of a borrower's disability, accident or illness, and unemployment. Credit life insurance has historically been among the most common bank insurance products.

Credit score. A number that is based on an analysis of an individual's credit history and that insurers may consider as an indicator of risk for purposes of underwriting insurance. Where not prohibited by state law, insurers may consider a person's credit history when underwriting personal lines.

Debt-cancellation contract/debt-suspension agreement. A loan term or contract between a lender and borrower whereby, for a fee, the lender agrees to cancel or suspend payment on the borrower's loan in the event of the borrowers's death, serious injury, unemployment, or other specified events. The Office of the Comptroller of the Currency considers these products to be banking products. State law determines whether these products are bank or insurance products for state-chartered banks and insurance companies.

Deductible. The amount a policyholder agrees to pay toward the total amount of insurance loss. The deductible may apply to each claim for a loss occurrence, such as each automobile accident, or to all claims made during a specified period, as with health insurance.

Directors and officers liability insurance. Liability insurance covering a corporation's obligation to reimburse its directors or officers for claims made against them for alleged wrongful acts. It also provides direct coverage for company directors and officers themselves in instances when corporate indemnification is not available.

Direct premiums written. Premiums received by an underwriter for all policies written during a given time period by the insurer, excluding those received through reinsurance assumed.

Direct writer. An insurance company that deals directly with the insured through a salaried representative, as opposed to those insurers that use agents. This term also refers to insurers that operate through exclusive agents. In reinsurance, a direct writer is the company that originally underwrites the insurance policies ceded.

Disability income insurance. An insurance product that provides income payment to the insured when his or her income is interrupted or terminated because of illness or accident.

Endowment insurance. A type of life insurance contract under which the insured receives the face value of the policy if he or she survives the endowment period. Otherwise, the beneficiary receives the face value of the policy upon the death of the insured.

Errors and omissions (E&O) liability insurance. Professional liability insurance that covers negligent acts or omissions resulting in loss. Insurance agents are continually exposed to the claim that inadequate or inappropriate coverage was recommended, resulting in a lack of coverage for losses incurred. The agent or the carrier may be responsible for coverage for legitimate claims.

Excess-of-loss reinsurance. A form of reinsurance whereby an insurer pays the amount of each claim for each risk up to a limit determined in advance, and the reinsurer pays the amount of the claim above that limit up to a specific sum. It includes various types of reinsurance, such as

catastrophe reinsurance, per-risk reinsurance, per-occurrence reinsurance, and aggregate excess-of-loss reinsurance.

Excess-per-risk reinsurance. A form of excess-of-loss reinsurance that, subject to a specified limit, indemnifies the ceding company against the amount of loss in excess of a specified retention for each risk involved in each occurrence.

Excess and surplus lines. Property/casualty coverage that is unavailable from insurers licensed by the state (admitted insurers) and must be purchased from a nonadmitted underwriter.

Exposure. The aggregate of all policyholder limits of liability arising from policies written.

Face amount. The amount stated on the face of the insurance policy to be paid, depending on the type of coverage, upon death or maturity. It does not include dividend additions or additional amounts payable under accidental death or other special provisions.

Facultative reinsurance. Reinsurance of individual risks by offer and acceptance wherein the reinsurer retains the faculty to accept or reject each risk offered by the ceding company.

Facultative treaty. A reinsurance contract under which the ceding company has the option to cede and the reinsurer has the option to accept or decline classified risks of a specific business line. The contract merely reflects how individual facultative reinsurance shall be handled.

Financial guarantee insurance. Financial guarantee insurance is provided for a wide array of financial risks. Typically, coverage is provided for the fulfillment of a specific financial obligation originated in a business transaction. The insurer, in effect, is lending the debtor its own credit rating to enhance the debtor's creditworthiness.

Financial strength rating. Opinion as to an insurance company's ability to meet its senior policyholder obligations and claims. For many years, the principal rating agency for property and casualty insurers and life insurers has been A.M. Best. Other rating agencies, such as Fitch, Moody's, Standard and Poor's, and Weiss, also rate insurers.

Fixed annuity. See *Annuity.*

Flood insurance. A special insurance policy to protect against the risk of loss or damage to property caused by flooding. Regular homeowners' policies do not pay for damages caused by flooding.

General liability insurance. A broad commercial policy that covers all business liability exposures, such as product liability, completed operations, premises and operations, independent contractors, and other exposures that are not specifically excluded.

Gross premiums written. Total premiums for insurance written during a given period, before deduction for reinsurance ceded.

Group insurance. Insurance coverage typically issued to an employer under a master policy for the benefit of employees. The insurer usually does not condition coverage of the people that make up the group upon satisfactory medical examinations or other requirements. The individual members of the group hold certificates as evidence of their insurance.

Health insurance. An insurance product that provides benefits for medical expenses incurred as a result of sickness or accident, as well as income payments to replace lost income when the insured is unable to work because of illness, accident, or disability. This product may be in the form of traditional indemnity insurance or managed-care plans and may be underwritten on an individual or group basis.

Incurred but not reported (IBNR). The loss-reserve value established by insurance and reinsurance companies in recognition of their liability for future payments on losses that have occurred but have not yet been reported to them. This definition is often erroneously expanded to include adverse loss development on reported claims. The term *incurred but not enough reported (IBNER)* is being increasingly used to reflect more accurately the adverse development on inadequately reserved reported claims.

Inland marine insurance. A broad field of insurance that covers cargo being shipped by air, truck, or rail. It includes coverage for most property involved in transporting cargo as well as for bridges, tunnels, and communications systems.

Key person life insurance. Life insurance designed to cover the key employees of an employer. It may be written on a group- or an individual-policy basis.

Lapse. The termination or discontinuance of a policy resulting from the insured's failure to pay the premium due.

Liability insurance. Protects policyholders from financial loss due to liability resulting from injuries to other persons or damage to their property.

Lines. A term used in insurance to denote insurance business lines, as in "commercial lines" and "personal lines."

Long-term care insurance. Health insurance designed to supplement the cost of nursing home care or other care facilities in the event of a long-term illness or permanent disability or incapacity.

Managing general agent. A managing general agent (MGA) is a wholesaler of insurance products and services to insurance agents. An MGA receives contractual authority from an insurer to assume many of the insurance company's functions. The MGA may provide insurance products to the public through local insurance agents as well as provide services to an insurance company, including marketing, accounting, data processing, policy maintenance, and claims-monitoring and -processing services. Many insurance companies prefer the MGA distribution and management system for their insurance products because it avoids the high cost of establishing branch offices. Most states require that an MGA be licensed.

Manuscript policy. A policy written to include specific coverage or conditions not provided in a standard policy.

Morbidity. The incidence and severity of illness and disease in a defined class of insured persons.

Mortality. The rate at which members of a group die in a specified period of time or die from a specific illness.

Mortgage guarantee insurance. A product that insures lenders against nonpayment by borrowers. The policies are issued for a specified time period. Lenders who finance more than 80 percent of the property's fair value generally require such insurance.

Mortgage insurance. Life insurance that pays the balance of a mortgage even if the borrower dies. Coverage typically is in the form of term life insurance, with the coverage declining as the debt is paid off.

Multiperil insurance. An insurance contract providing coverage against many perils, usually combining liability and physical damage coverage.

Net premiums written. The amount of gross premiums written, after deduction for premiums ceded to reinsurers.

Ninety-day loss rule. A state requirement for an insurer to establish a loss provision for reinsurance recoverables over 90 days past due.

Obligatory treaty. A reinsurance contract under which business must be ceded in accordance with contract terms and must be accepted by the reinsurer.

Policyholder. The person or entity who owns an insurance policy. This is usually the insured person, but it may also be a relative of the insured, a partnership, or a corporation.

Premium. The payment, or one of the periodic payments, a policyholder agrees to make for insurance coverage.

Private mortgage insurance (PMI). Coverage for a mortgage lender against losses due to a collateral shortfall on a defaulted residential real estate loan. Most banks require borrowers to take out a PMI policy if a downpayment of less than 20 percent of a home's value is made at the time the loan is originated. PMI does not directly benefit a borrower, although its existence provides the opportunity to purchase a home to many people who otherwise would not qualify for a loan.

Producer. A person licensed to sell, solicit, or negotiate insurance.

Professional designations and organizations. Three of the most common insurance professional designations are chartered life under-

writer (CLU), chartered property casualty underwriter (CPCU), and chartered financial consultant (ChFC). Insurance agents also join professional organizations such as the American Society of Chartered Life Underwriters, the International Association of Financial Planning, the National Association of Life Underwriters, the National Association of Health Underwriters, the American Council of Life Insurance, the Life Insurance Marketing and Research Association, the Life Underwriter Training Council, and the Million Dollar Round Table.

Pro rata reinsurance. A generic term describing all forms of ''quota-share'' and ''surplus reinsurance,'' in which the reinsurer shares a pro rata portion of the losses and premiums of the ceding company.

Property insurance. Coverage for physical damage or destruction of real property (buildings, fixtures, and permanently attached equipment) and personal property (movable items that are not attached to land) that occurs during the policy period as a result of, for example, fire, windstorm, explosion, or vandalism.

Protected cell. A structure available to captive insurers underwriting risks of unaffiliated companies whereby the assets associated with the self-insurance program of one organization are segregated to provide legal-recourse protection from creditors of protected cells providing insurance coverage to other organizations.

Quota-share reinsurance. A form of pro rata reinsurance indemnifying the ceding company for a fixed percent of loss on each risk covered in the contract in consideration of the same percentage of the premium paid to the ceding company.

Rebating. Directly or indirectly giving or offering to give any portion of the premium or any other consideration to an insurance buyer as an inducement to purchase or renew the insurance. Rebates are forbidden under most state insurance codes.

Reinsurance. Insurance placed by an underwriter (the ceding company or reinsured) in another company to transfer or reduce the amount of the risk assumed under the original insurance policy (or group of policies).

Reinsurance premium. The consideration paid by a ceding company to a reinsurer for the coverage provided by the reinsurer.

Residual market. Also known as the shared market, it covers applications for insurance that were rejected by underwriters in the voluntary market that is covered by agency direct-marketing systems, perhaps because of high loss experience by the insured party. The residual market includes government insurance programs, specialty pools, and shared market mechanisms such as assigned-risk plans.

Retrocession. A reinsurance transaction whereby a reinsurer (the retrocedant) cedes all or part of the reinsurance risks it has assumed to another reinsurer (the retrocessionaire).

Retrospective rating. An insurance plan in which the current year's premium is based on the insured's own loss experience for that same period, subject to a maximum and minimum.

Rider. A written attachment, also known as an endorsement, to an insurance policy that changes the original policy to meet specific requirements, such as increasing or decreasing benefits or providing coverage for specific property items beyond that provided for under the insurance company's standard contract terms.

Self-insured retention (SIR). The percentage of a risk or potential loss assumed by an insured, whether in the form of a deductible, self-insurance, or no insurance at all.

Separate accounts. Certain life insurance assets and related liabilities that are segregated and maintained to meet specific investment objectives of contract holders, particularly those assets and liabilities associated with pension plans and variable products offered by life insurers, wherein the customer and not the insurer retains most of the investment and interest-rate risk.

Split-dollar life insurance. An arrangement that typically involves an agreement between an employer and an employee whereby the premium payment, cash values, policy ownership, and death benefits may be split. There are many variations of split-dollar arrangements, including arrangements in which a trust is created to facilitate estate planning. Split-dollar life insurance is designed to serve as a supplemental

benefit to a particular company executive. The arrangement typically involves the payment of the insurance premium by the employer, with the death benefit accruing to the employee.

Subrogation. An insurance carrier may reserve the "right of subrogation" in the event of a loss. This means that the company may choose to take action to recover the amount of a claim paid to a covered insured if a third party caused the loss. After expenses, the amount recovered must be divided proportionately with the insured to cover any deductible for which the insured was responsible.

Term life insurance. An insurance product that provides, for a specified period of time, death coverage only. Typically, it has no savings component and, therefore, no cash value. Because term insurance provides only mortality protection, it generally provides the most coverage per premium dollar. Most term life insurance policies are renewable for one or more time periods up to a stipulated maximum age; however, premiums generally increase with the age of the policyholder.

Title insurance. Insurance that protects banks and mortgagees against unknown encumbrances against real estate by indemnifying the mortgagor and property owner in the event that clear ownership of the property is clouded by the discovery of faults in the title. Title insurance policies may be issued to either the mortgagor or the mortgagee or both. Title insurance is written largely only by companies specializing in this class of insurance.

Treaty reinsurance. A reinsurance contract under which the reinsured company agrees to cede, and the reinsurer agrees to assume, risks of a particular class or classes of business.

Twisting. In insurance, twisting involves making misrepresentations to a policyholder to induce the policyholder to terminate one policy and take out another policy with another company, when it is not to the insured's benefit. Twisting is a violation of the Unfair Trade Practices Act. Twisting is similar to the "churning" concept in securities sales, and it results in increased commissions for the inducing agent.

Umbrella liability insurance. This type of liability insurance provides excess liability protection over the "underlying" liability insurance coverage to supplement underlying policies that have been reduced or exhausted by loss.

Underwriting. The process by which a company determines whether it can accept an application for insurance and by which it may charge an appropriate premium for those applications selected. For example, the underwriting process for life insurance classifies applicants by identifying such characteristics as age, sex, health, and occupation.

Unearned reinsurance premium. The part of the reinsurance premium that is applicable to the unexpired portion of the policies reinsured.

Universal life insurance. A form of permanent insurance designed to provide flexibility in premium payments and death benefit protection. The policyholder can pay maximum premiums and maintain a high cash surrender value. Alternatively, the policyholder can make minimal payments in an amount only large enough to cover mortality and other expense charges.

Variable annuity. See *Annuity.*

Variable life insurance. A form of whole life, or universal life, insurance in which the policyholder's cash value is invested in "separate accounts" of the insurer. These accounts are segregated from the insurance carrier's other asset holdings. Such separate account investments are generally not available to a carrier's general creditors in the event of the carrier's insolvency. The policyholder assumes the investment and price risk. Because variable life policies have investment features, life insurance agents selling these policies must be registered representatives of a broker-dealer licensed by the Financial Industry Regulatory Authority and registered with the Securities and Exchange Commission.

Vendors' single-interest insurance. A form of force-placed insurance that is typically purchased by the bank to protect against loss or damage to loan collateral in which the bank has a security interest. The bank passes its expense for this insurance on to the consumer who has either refused or is unable to obtain property insurance.

Viatical settlement. The cashing in of a life insurance policy at a discount from face amount

by policyholders who are often terminally ill and need the money for medical care. The purchaser becomes the policyholder as well as the beneficiary and assumes the premium payments of the policy.

Whole life insurance. A fixed-rate insurance product, with premiums and death benefits guaranteed over the duration of the policy. There is a cash value (essentially a savings account) that accrues to the policyholder tax deferred. A policyholder receives the cash value in lieu of death benefits if the policy matures or lapses before the insured's death. A policyholder also may borrow against the policy's accumulated cash value or use it to pay future premiums. For most whole life insurance policies, premiums are constant for the life of the insured's contract.

Insurance Sales Activities and Consumer Protection in Sales of Insurance

Examination Objectives

Effective date November 2003

Section 4043.2

1. To understand the volume and complexity of the state member bank's insurance or annuity program and insurance sales strategy.
2. To assess the financial results of the insurance and annuity sales activity compared with planned results.
3. To determine if the state member bank's insurance and annuity sales activities are effectively integrated into the risk-management, audit, and compliance functions and if the control environment is adequate.
4. To assess the adequacy of the state member bank's controls to ensure compliance with the applicable state and federal laws and regulations.
5. To assess the state member bank's level and direction of operational, legal, and reputational risks from the insurance or annuity sales activity.

The following objectives apply if insurance products or annuities are sold by a bank or another person at an office of, or on behalf of, the bank.

6. To assess the adequacy of the state member bank's oversight program for ensuring compliance with the Consumer Protection in Sales of Insurance (CPSI) regulation. (See section 4043.1.)
7. To assess the effectiveness of the state member bank's audit and compliance programs for the CPSI regulation.
8. To assess the state member bank's current compliance with the CPSI regulation.
9. To obtain commitments for corrective action when the state member bank is in violation of the CPSI regulation or when applicable policies, procedures, practices, or management oversight to protect against violations is deficient.

RISK ASSESSMENT OF INSURANCE AND ANNUITY SALES ACTIVITIES

The examiner should consider the following procedures, as appropriate, when conducting a risk assessment to determine the level and direction of risk exposure to the state member bank that is attributable to insurance or annuity sales activity. If there are specific areas of concern, the examiner should focus primarily on those areas.

1. *Scope of activities and strategies.* Assess the significance and complexity of the insurance or annuity sales program.
   a. Obtain a general overview of the scope of the state member bank's insurance or annuity sales activities and any anticipated or recent change in or expansion of such activities.
   b. Determine the state member bank's strategy for insurance or annuity sales, including strategies for cross-selling and referrals of insurance and banking products. Determine the institution's experience with any cross-marketing programs for both insurance business generated by the bank and bank business generated by insurance producers.
   c. Obtain two years' worth of income statements, balance sheets, and budget documents for the agency's activities. Compare the expected budget items with their actual results.
   d. Determine the volume and type of insurance or annuity products and services sold or solicited.
   e. Determine what other related services the state member bank provides in connection with its insurance or annuity sales activities, such as providing risk-management services to clients seeking advice on appropriate insurance coverages, claims processing, and other activities.
2. *Insurance sales products and concentrations.*
   a. Determine the composition of sales—
      - by line of business, such as property/casualty insurance, life insurance including annuities, and health insurance;
      - by the proportion of sales to commercial and retail customers; and
      - by the portion of sales that is credit related, such as credit life and credit health insurance.
   b. Determine any sales concentrations to particular entities, industries, or bank customers.
   c. Note any concentrations to large commercial accounts.
   d. Determine what insurance services are provided to the bank, its employees, and bank affiliates.
3. *Legal-entity and risk-management structure for insurance or annuity sales.*
   a. Obtain an organizational chart for the legal-entity and risk-management structure for the insurance or annuity sales activities.
   b. Determine—
      - whether the insurance or annuity sales activity is conducted in an affiliated producer, by the bank itself, through another distribution arrangement, or by a combination of these arrangements;
      - the names of any affiliated insurance agencies and the states where the affiliated insurance agencies are licensed;
      - the locations outside of the United States where insurance or annuities are sold or solicited; and
      - if any subsidiary agency operates as a financial subsidiary under the Gramm-Leach-Bliley Act.
   c. Determine if the insurance or annuity producer is acting as a managing general agent (MGA).[1] If so, determine—
      - the scope of the MGA activities;
      - the state member bank management's

1. MGAs do not assume underwriting risk. Through contractual arrangements with an insurer, MGAs have the authority to write policies on behalf of the insurer in certain instances, thereby binding the insurer to the policy. Certain minimum provisions governing MGA agreements are delineated in the applicable National Association of Insurance Commissioners (NAIC) model law.

assessment of the risk associated with the MGA activity; and
- what risk controls are in place to protect the state member bank from potential loss that may arise from the MGA's activities, such as loss arising from legal liability.

4. *Strategic and financial plans.* Assess management controls over the insurance and annuity sales activities.
   a. Ascertain the state member bank management's strategic and financial plans and goals for the insurance or annuity sales activity.
   b. Review the state member bank's due-diligence process for acquiring and pricing agencies, if applicable.
   c. Review the state member bank's financial budgets and forecasts for the activity, particularly plans for new products, marketing strategies and marketing arrangements, and the rate of actual and expected growth for the activity.
   d. Determine the cause for significant deviations from the plan.
   e. Determine if any agency acquired by the state member bank is providing the expected return on investment and if the agency's revenues are covering the debt servicing associated with the purchase, if applicable.
5. *Review of board and committee records and reports.*
   a. Review the reports of any significant state member bank oversight committees, including relevant board of directors and board committee minutes and risk-management reports.
   b. Determine if the board of directors, a board committee, or senior management of the state member bank reviews reports pertaining to consumer complaints and complaint resolution, information pertaining to litigation and associated losses, and performance compared with the organization's plan for the insurance and annuity sales activities.
6. *Policies and procedures.*
   a. Determine—
      - the adequacy of the state member bank's policies and procedures for conducting and monitoring insurance or annuity sales activities, including those policies designed to ensure adherence with federal and state laws and regulations pertaining to consumer protection;
      - whether there are appropriate policies and procedures for the handling of customer funds collected on behalf of the underwriter; accurate and timely financial reporting; complaint monitoring and resolution; effective system security and disaster-recovery plans; and policy-exception tracking and reporting; and
      - if the board of directors or its designated committee has formally approved the policies.
   b. Obtain a detailed balance sheet for agency subsidiaries, and determine if the assets held by insurance or annuity agency subsidiaries of the state member bank are all bank-eligible investments.
   c. Determine the independence of the state member bank's audit program applicable to the insurance and annuity sales activity. Determine if the audit program's scope, frequency, and resources are commensurate with the insurance or annuity sales activities conducted.
   d. Determine how the state member bank selects insurance underwriters with whom to do business, as well as how the state member bank monitors the continuing performance of the underwriters.
   e. Determine the adequacy of the oversight of the bank's board of directors over the insurance management team's qualifications, the training and licensing of personnel, and general compliance with state insurance regulations.
   f. Review the internal controls of the state member bank related to third-party arrangements, including arrangements for sales, processing, and auditing of insurance or annuity sales activities.
7. *Claims, litigation, and functional regulatory supervision.* Assess legal and reputational risk.
   a. Identify any significant litigation against the state member bank arising from its insurance or annuity sales activity and the likely impact of the litigation on the state member bank.
   b. Obtain the insurance agency's errors and omissions claims records for the past several years, including a listing of claims it has made and the amount of claims, the

claim status, and the amount of claim payments.

c. Review the state member bank's policies and procedures for tracking and resolving claims. Determine if they appear adequate and if they are adhered to.

d. Determine if the applicable functional regulator has any outstanding supervisory issues with the insurance agency.

8. *Consumer complaints.*

a. Determine if bank managagement has policies and procedures in place to assess whether consumer complaints received are likely to expose the state member bank to regulatory action, litigation, reputational damage, or other significant risk.

b. Obtain applicable consumer complaint files, and evaluate internal control procedures to ensure the complaints are being adequately addressed.

9. *Audit and compliance functions.*

a. Determine the date of the most recent review of the insurance or annuity sales activities by the audit and compliance functions.

b. Determine the adequacy of the state member bank's management policies and procedures for ensuring that any deficiencies noted in such reviews are corrected, and ascertain whether any such deficiencies are being adequately addressed.[2]

10. *Insurance underwriter oversight of agent/agency activities.*

a. Determine if there are adequate policies and procedures to review and resolve any issues or concerns raised by an insurance underwriter regarding the producers used by, or affiliated with, the state member bank.[3]

b. Determine whether any of the insurance underwriters conducted a periodic review of the producers that they engaged to sell insurance.

11. *State supervisory insurance authorities.*

a. During discussions with state member bank management, determine whether state insurance regulators have raised any issues or concerns in correspondence or reports.

b. Consult with the state insurance regulators, as appropriate, to determine any significant supervisory issues, actions, or investigations. (For multistate agencies, contacts with states may be prioritized on the basis of the location of the agency's head office or by a determination of the significance of sales by state. Both financial examinations and market conduct examinations conducted by the state insurance departments are targeted at insurance underwriters, not agencies. Therefore, information available from the states pertaining to agencies may be very limited.)

12. *Operational risk assessment.* Ascertain from the state member bank's management whether there are—

a. any significant operational problems or concerns relating to insurance or annuity sales activities;

b. policies and procedures in place to ensure accurate and timely reporting to the state member bank's management of insurance or annuity sales activity plans, financial results, and significant consumer complaints or lawsuits or compliance issues, such as errors and omissions claims;[4]

c. appropriate policies and procedures at the state member bank to ensure accurate reporting of insurance or annuity sales activity on Federal Reserve regulatory reports (Determine from applicable Board or Reserve Bank contacts if there are any outstanding issues with respect to potential reporting errors on submitted Federal Reserve reports, bank call reports, or other applicable reports. If so, seek resolution of the issues.); and

d. adequate disaster-recovery plans and procedures to protect the state member bank

2. Enforcement of the privacy provisions of the Gramm-Leach-Bliley Act as they relate to state member banks is the responsibility of the Board's Division of Consumer and Community Affairs. However, enforcement of the privacy provisions of the GLB Act with respect to the insurance activities of nondepository subsidiaries of a state member bank is the responsibility of the state insurance regulators.

3. Insurance underwriters generally have procedures to determine whether individual producers affiliated with agencies are selling the underwriters' products in conformance with applicable laws and regulations. The findings and conclusions of these reviews should be available to the state member bank's management.

4. Errors and omissions insurance should be in place to protect the state member bank against loss sustained because of an error or oversight, such as failure to issue an insurance policy. A tracking system to monitor errors and omission claims should be in place and monitored by the state member bank, as appropriate. See section 4040.1, "Management of Insurable Risks."

from loss of data related to insurance or annuity sales activities.

CONSUMER PROTECTION IN SALES OF INSURANCE REGULATION

The following procedures should be risk-focused in accordance with the Federal Reserve's risk-focused framework for supervising banking organizations. The procedures should be carried out as necessary to adequately assess the state member bank's compliance with the Consumer Protection in Sales of Insurance (CPSI) regulation.

1. Determine the role of the state member bank's board of directors and management in ensuring compliance with the CPSI regulation and applicable state consumer regulations.
2. Evaluate the management information system (MIS) reports the state member bank's board or designated committee rely on to monitor compliance with the consumer regulations and to track complaints and complaint resolution.
3. Review the state member bank's policies and procedures to ensure they are consistent with the CPSI regulation, and conduct transaction testing, as necessary, in the following areas.[5]
   a. disclosures, advertising, and promotional materials
   b. consumer acknowledgments
   c. physical separation from areas of deposit-taking activities
   d. qualifications and licensing for insurance personnel
   e. compliance programs and internal audits
   f. hiring, training, and supervision of insurance or annuity sales personnel employed directly by the bank, or of third parties selling insurance or annuity products at a state member bank office or on behalf of the state member bank
   g. compensation practices and training for personnel making referrals
4. If a third party sells insurance or annuities at the state member bank's offices, or on behalf of the bank, review the state member bank's policies and procedures for ensuring that the third party complies with the CPSI regulation and other relevant policies and procedures of the bank.
5. Review the bank's process for identifying and resolving consumer complaints related to the sale of insurance products and annuities.
6. Obtain and review the record of consumer complaints related to the CPSI regulation. (These records are available from the Board's Division of Consumer and Community Affairs database. See CP letter 2001-11.)
7. Include examination findings, as appropriate, in the commercial bank examination report or in other communications to the bank, as appropriate, that pertain to safety-and-soundness reviews of the bank.

5. If the examiner determines that transaction testing of a functionally regulated nonbank affiliate of the state member bank is appropriate in order to determine the state member bank's compliance with the CPSI regulation, the examiner should first consult with and obtain approval from appropriate staff of the Board's Division of Banking Supervision and Regulation.

Insurance Sales Activities and Consumer Protection in Sales of Insurance

Internal Control Questionnaire

Effective date November 2003

Section 4043.4

RISK ASSESSMENT OF INSURANCE AND ANNUITY SALES ACTIVITIES

Program Management

1. Does the state member bank have a comprehensive program to ensure that its insurance and annuity sales activities are conducted in a safe and sound manner?
2. Does the state member bank have appropriate written policies and procedures commensurate with the volume and complexity of the insurance or annuity sales activities?
3. Has bank management obtained the approval of the bank's board of directors for the program scope and the associated policies and procedures?
4. Have reasonable precautions been taken to ensure that disclosures to customers for insurance or annuity sales and solicitations are complete and accurate, and are in compliance with applicable laws and regulations?
5. Does the state member bank effectively oversee the insurance or annuity sales activities, including those involving third parties?
6. Does the state member bank have an effective independent internal audit and compliance program in place to monitor retail sales of insurance or annuity products?
7. Does the bank appropriately train and supervise employees conducting insurance or annuity sales activities?

Management Information Systems

8. Does the state member bank's insurance program management plan establish the appropriate management information systems (MIS) necessary for the board of directors to properly oversee the bank's insurance or annuity sales activities?
9. Does MIS provide sufficient information to allow for the evaluation and measurement of the effect of actions taken to identify, track, and resolve any issues relative to compliance with the Consumer Protection in Sales of Insurance (CPSI) regulation?
10. Does MIS include sales volumes and trends, profitability, policy exceptions and associated controls, customer complaints, and other information providing evidence of compliance with laws and established policies?

Compliance Programs and Internal Audits

11. Are there policies and procedures in place to ensure that insurance or annuity sales activities are conducted in compliance with applicable laws and regulations?
12. Do compliance procedures identify potential conflicts of interest and how such conflicts should be addressed?
13. Do the compliance procedures provide a system to monitor customer complaints and track their resolution?
14. When applicable, do compliance procedures call for verification that third-party sales are being conducted in a manner consistent with the agreement governing the third party's arrangement with the state member bank?
15. Is the compliance function conducted independently of the insurance or annuity sales and management activities?
16. Do compliance personnel determine the scope and frequency of the insurance-product review?
17. Are findings of insurance or annuity sales activity compliance reviews periodically reported directly to the state member bank's board of directors or a designated committee thereof?

CONSUMER PROTECTION IN SALES OF INSURANCE REGULATION

If applicable, review the state member bank's internal controls, policies, practices, and proce-

dures for retail insurance or annuity sales activities conducted by the bank on bank premises or on behalf of the bank. The bank's program management for such activities should be well documented and should include appropriate personnel training, as well as compliance and audit-function coverage of all efforts to ensure compliance with the provisions of the Board's CPSI regulation.

Advertising and Promotional Materials

1. Do advertising materials associated with the insurance or annuity sales program create an erroneous belief that—
   a. an insurance product or annuity sold or offered for sale by the state member bank, or on behalf of the bank, is backed by the federal government or the bank, or that the product is insured by the FDIC?
   b. an insurance product or annuity that involves investment risk does not, in fact, have investment risk, including the potential that principal may be lost and the product may decline in value?
2. Does a review of advertising for insurance products or annuities sold or offered for sale create an erroneous impression that—
   a. the state member bank or an affiliate or subsidiary may condition the grant of an extension of credit to a consumer on the purchase of an insurance product or annuity by the consumer from the bank or an affiliate or subsidiary of the bank?
   b. the consumer is not free to purchase an insurance product or annuity from another source?

Disclosures

3. In connection with the initial purchase of an insurance product or annuity by a consumer, does the initial disclosure to the consumer, except to the extent the disclosure would not be accurate, state that—
   a. the insurance product or annuity is not a deposit or other obligation of, or is not guaranteed by, the state member bank or an affiliate of the bank?
   b. the insurance product or annuity is not insured by the FDIC or any other agency of the United States, the state member bank, or (if applicable) an affiliate of the bank?
   c. in the case of an insurance product or annuity that involves an investment risk, there is risk associated with the product, including the possible loss of value?
4. In the case of an application for credit, in connection with which an insurance product or annuity is solicited, offered, or sold, is a disclosure made that the state member bank may not condition an extension of credit on either—
   a. the consumer's purchase of an insurance product or annuity from the bank or any of its affiliates?
   b. the consumer's agreement not to obtain, or a prohibition on the consumer's obtaining, an insurance product or annuity from an unaffiliated entity?
5. Are the disclosures under question 3 above provided orally and in writing before the completion of the initial face-to-face sale of an insurance product or annuity to a consumer?
6. Are the disclosures under question 4 above made orally and in writing at the time the consumer applies in a face-to-face interaction for an extension of credit in connection with which insurance is solicited, offered, or sold?
7. If a sale of an insurance product or annuity is conducted by telephone, are the disclosures under question 3 above provided in writing, by mail, within three business days?
8. If an application for credit is by telephone, are the disclosures under question 4 above provided by mail to the consumer within three business days?
9. Are the disclosures under questions 3 and 4 above provided through electronic media, instead of on paper, only if the consumer affirmatively consents to receiving the disclosures electronically, and only if the disclosures are provided in a format that the consumer may retain or obtain later?
10. Are disclosures made through electronic media, for which paper or oral disclosures are not required, presented in a meaningful form and format?
11. Are disclosures conspicuous, simple, direct, readily understandable, and designed to call attention to the nature and significance of the information provided?

12. Are required disclosures presented in a meaningful form and format?

Consumer Acknowledgment

13. At the time a consumer receives the required disclosures, or at the time of the consumer's initial purchase of an insurance product or annuity, is a written acknowledgment from the consumer that affirms receipt of the disclosures obtained?
14. If the required disclosures are provided in connection with a transaction that is conducted by telephone—
    a. has an oral acknowledgment of receipt of the disclosures been obtained, and is sufficient documentation maintained to show that the acknowledgment was given?
    b. have reasonable efforts to obtain a written acknowledgment from the consumer been made?

Physical Separation from Deposit Activities

15. Does the state member bank, to the extent practicable—
    a. keep the area where the bank conducts transactions involving the retail sale of insurance products or annuities physically segregated from the areas where retail deposits are routinely accepted from the general public?
    b. identify the areas where insurance product or annuity sales activities occur?
    c. clearly delineate and distinguish insurance and annuity sales areas from the areas where the bank's retail deposit-taking activities occur?

Qualifications and Licensing

16. Does the state member bank permit any person to sell, or offer for sale, any insurance product or annuity in any part of its office, or on its behalf, only if the person is at all times appropriately qualified and licensed under applicable state insurance licensing standards for the specific products being sold or recommended?

Hiring, Training, and Supervision

17. Have background investigations of prospective employees that will sell insurance products or annuities been completed?
18. When a candidate for employment has previous insurance experience, has a review to determine whether the individual has been the subject of any disciplinary actions by state insurance regulators been completed?
19. Do all insurance or annuity sales personnel, or third-party sales personnel conducting sales activities at or on behalf of the state member bank, receive appropriate training and continue to meet licensing requirements?
20. Does training address policies and procedures for sales of insurance and annuity products, and does it cover personnel making referrals to a licensed insurance producer?
21. Does training ensure that personnel making referrals about insurance products or annuities are properly handling all inquiries so as not to be deemed to be acting as unlicensed insurance agents or registered (or equivalently trained) securities sales representatives (for insurance products that are also securities) if they are not qualified?
22. When insurance products or annuities are sold by the state member bank or third parties at an office of, or on behalf of, the organization, does the institution have policies and procedures to designate, by title or name, the individuals responsible for supervising insurance sales activities, as well as the referral activities of bank employees not authorized to sell these products?
23. Does the bank designate supervisory personnel responsible for monitoring compliance with any third-party agreement, as well as with the CPSI regulation?

Referrals

24. Are fees paid to nonlicensed personnel who are making referrals to qualified insurance or annuity salespersons limited to a one-time, nominal fee of a fixed dollar amount for each referral, and is the fee unrelated to whether the referral results in a sales transaction?

Third-Party Agreements

25. Does the state member bank's management conduct a comprehensive review of a third party before entering into any arrangement to conduct insurance or annuity sales activities through the third party?
26. Does the review include an assessment of the third party's financial condition, management experience, reputation, and ability to fulfill its contractual obligations to the bank, including compliance with applicable consumer protection laws and regulation?
27. Does the board of directors or a designated committee thereof approve any agreement with the third party?
28. Does the agreement outline the duties and responsibilities of each party; describe the third-party activities permitted on the institution's premises; address the sharing or use of confidential customer information; and define the terms for use of the bank's office space, equipment, and personnel?
29. Does the third-party agreement specify that the third party will comply with all applicable laws and regulations and will conduct its activities in a manner consistent with the CPSI regulation, if applicable?
30. Does the agreement authorize the bank to monitor a third party's compliance with the agreement, as well as to have access to third-party records considered necessary to evaluate compliance?
31. Does the agreement provide for indemnification of the institution by the third party for any losses caused by the conduct of the third party's employees in connection with its insurance or annuity sales activities?
32. If an arrangement includes dual employees, does the agreement provide for written employment contracts that specify the duties of these employees and their compensation arrangements?
33. If the state member bank contracts with a functionally regulated third party, does the bank obtain, as appropriate, any relevant regulatory reports of examination of the third party?
34. How does the state member bank ensure that a third party selling insurance or annuity products at or on behalf of the bank complies with all applicable regulations, including the CPSI regulation?
35. How does the state member bank ensure that any third party or dual employee selling insurance or annuity products at or on behalf of the bank is appropriately trained to comply with the minimum disclosures and other requirements of the Board's CPSI regulation and applicable state regulations?
36. Does the bank obtain and review copies of third-party training and compliance materials to monitor the third party's performance regarding its disclosure and training obligations?

Consumer Complaints

37. Does the state member bank have policies and procedures for handling customer complaints related to insurance and annuity sales?
38. Does the customer complaint process provide for the recording and tracking of all complaints?
39. Does the state member bank require periodic reviews of complaints by compliance personnel? Is a review by the state member bank's board and senior management required for significant compliance issues that may pose risk to the state member bank?

Banking organizations increasingly rely on information technology (IT) to conduct their operations and manage risks. The use of IT can have important implications for a banking organization's financial condition, risk profile, and operating performance and should be incorporated into the safety-and-soundness assessment of each organization. As a result, all safety-and-soundness examinations (or examination cycles) conducted by the Federal Reserve should include an assessment and evaluation of IT risks and risk management. Further information about banks' IT activities and examination methodology can be found in the *FFIEC Information Technology Examination Handbook* (the *IT Handbook*) and in supervisory guidance issued by the Federal Reserve and the other federal banking agencies.

ASSESSING INFORMATION TECHNOLOGY IN THE RISK-FOCUSED SUPERVISORY FRAMEWORK

The risk-focused supervisory process is evolving to adapt to the changing role of IT in banking organizations, with greater emphasis on an assessment of IT's effect on an organization's safety and soundness. Accordingly, examiners should explicitly consider IT when developing risk assessments and supervisory plans. Examiners should use appropriate judgment in determining the level of review, given the characteristics, size, and business activities of the organization. Moreover, to determine the scope of supervisory activities, close coordination is needed between general safety-and-soundness examiners and IT specialists during the risk-assessment and planning phase, as well as during on-site examinations. Given the variability of IT environments, the level of technical expertise needed for a particular examination will vary across institutions and should be identified during the planning phase of the examination. In general, examiners should accomplish the following goals during a risk-focused examination:

- Develop a broad understanding of the organization's approach to, and strategy and structure for, IT activities within and across business lines. Determine also the role and importance of IT to the organization and any unique characteristics or issues.
- Incorporate an analysis of IT activities into risk assessments, supervisory plans, and scope memoranda. An organization's IT systems should be considered in relation to the size, activities, and complexity of the organization, as well as the degree of reliance on these systems across particular business lines. Although IT concerns would clearly affect an institution's operational risk profile, IT also can affect other business risks (such as credit, market, liquidity, legal, and reputational risk), depending upon the specific circumstances, and should be incorporated into these assessments as appropriate.
- Assess the organization's critical systems, that is, those that support its major business activities, and the degree of reliance those activities have on IT systems. The level of review should be sufficient to determine that the systems are delivering the services necessary for the organization to conduct its business in a safe and sound manner.
- Determine whether the board of directors and senior management are adequately identifying, measuring, monitoring, and controlling the significant risks associated with IT for the overall organization and its major business activities.

INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

The federal banking agencies jointly issued interagency guidelines establishing information security standards (the information security standards), which became effective July 1, 2001.[1] (See the appendix to this section.) The Board of Governors of the Federal Reserve System approved amendments to the standards on December 16, 2004 (effective July 1, 2005). The amended information security standards implement sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) and section 216 of the Fair and Accurate Credit

1. See 66 Fed. Reg. 8616–8641 (February 1, 2001) and 69 Fed. Reg. 77,610–77,612 (December 28, 2004); Regulation H, 12 CFR 208, appendix D-2; Regulation K, 12 CFR 211.9 and 211.24; and Regulation Y, 12 CFR 225, appendix F.

Transactions Act of 2003 (15 U.S.C. 1681w). The Gramm-Leach-Bliley Act requires the agencies to establish financial-institution information security standards for administrative, technical, and physical safeguards for customer records and information. (See SR-01-15.)

Under the information security standards, institutions must establish an effective *written* information security program to assess and control risks to customer information. An institution's information security program should be appropriate to its size and complexity and to the nature and scope of its operations. The board of directors should oversee the institution's development, implementation, and maintenance of the information security program and also approve written information security policies and programs.

The information security program should include administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. The program should be designed to ensure the security and confidentiality of customer information;[2] protect against anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to, or use of, such information that could result in substantial harm or inconvenience to any customer;[3] and ensure the proper disposal of customer information and consumer information. Each institution must assess risks to customer information and implement appropriate policies, procedures, training, and testing to manage and control these risks. Institutions must also report annually to the board of directors or a committee of the board of directors.

The information security standards outline specific security measures that banking organizations should consider in implementing a security program based on the size and complexity of their operations. Training and testing are also critical components of an effective information security program. Financial institutions are required to oversee their service-provider arrangements in order to (1) protect the security of customer information maintained or processed by service providers; (2) ensure that its service providers properly dispose of customer and consumer information; and (3) where warranted, monitor its service providers to confirm that they have satisfied their contractual obligations.

The Federal Reserve recognizes that banking organizations are highly sensitive to the importance of safeguarding customer information and the need to maintain effective information security programs. Existing examination procedures and supervisory processes already address information security. As a result, most banking organizations may not need to implement any new controls and procedures.

Examiners should assess compliance with the standards during each safety-and-soundness examination, which may include targeted reviews of information technology. Ongoing compliance with the standards should be monitored, as needed, during the risk-focused examination process. Material instances of noncompliance should be noted in the examination report.

The information security standards apply to customer information maintained by, or on behalf of, state member banks and bank holding companies and the nonbank subsidiaries of each.[4] The information security standards also address standards for the proper disposal of consumer information, pursuant to sections 621 and 628 of the Fair Credit Reporting Act (15 U.S.C. 1681s and 1681w). To address the risks associated with identity theft, a financial institution is generally required to develop, implement, and maintain, as part of its existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports.

Consumer information is defined as any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report and that is maintained or otherwise possessed by or on

2. *Customer information* is defined to include any record, whether in paper, electronic, or other form, containing *nonpublic personal information*, as defined in Regulation P, about a financial institution's customer that is maintained by, or on behalf of, the institution.

3. A *customer* is defined in the same manner as in Regulation P: a consumer who has established a continuing relationship with an institution under which the institution provides one or more financial products or services to the consumer to be used primarily for personal, family, or household purposes. The definition of customer does not include a business, nor does it include a consumer who has not established an ongoing relationship with the financial institution.

4. The information security standards do not apply to brokers, dealers, investment companies, and investment advisers, or to persons providing insurance under the applicable state insurance authority of the state in which the person is domiciled. The appropriate federal agency or state insurance authority regulates insurance entities under sections 501 and 505 of the GLB Act.

behalf of the bank for a business purpose. Consumer information also means a compilation of such records.

The following are examples of consumer information:

- a consumer report that a bank obtains
- information from a consumer report that the bank obtains from its affiliate after the consumer has been given a notice and has elected not to opt out of that sharing
- information from a consumer report that the bank obtains about an individual who applies for but does not receive a loan, including any loan sought by an individual for a business purpose
- information from a consumer report that the bank obtains about an individual who guarantees a loan (including a loan to a business entity)
- information from a consumer report that the bank obtains about an employee or prospective employee

Consumer information does not include any record that does not personally identify an individual, nor does it include the following:

- aggregate information, such as the mean score, derived from a group of consumer reports
- blind data, such as payment history on accounts that are not personally identifiable, that may be used for developing credit scoring-models or for other purposes
- information from a consumer report that the bank obtains about an individual who applies for but does not receive a loan, including any loan sought by an individual for a business purpose
- information from a consumer report that the bank obtains about an individual who guarantees a loan (including a loan to a business entity)
- information from a consumer report that the bank obtains about an employee or prospective employee

An institution or banking organization is not required to implement a *uniform* information security program. For example, a bank holding company may include subsidiaries within the scope of its information security program, or the subsidiaries may implement separate information security programs. The institution or bank holding company is expected, however, to coordinate all the elements of its information security program.

Institutions must exercise due diligence when selecting service providers, including reviewing the service provider's information security program or the measures the service provider uses to protect the institution's customer information.[5] All contracts must require that the service provider implement appropriate measures designed to meet the objectives of the standards. Institutions must also conduct ongoing oversight to confirm that the service provider maintains appropriate security measures. An institution's methods for overseeing its service-provider arrangements may differ depending on the type of services or service provider or the level of risk. For example, if a service provider is subject to regulations or a code of conduct that imposes a duty to protect customer information consistent with the objectives of the standards, the institution may consider that duty in exercising its due diligence and oversight of the service provider. In situations where a service provider hires a subservicer (or subcontractor), the subservicer would not be considered a "service provider" under the guidelines.

Response Programs for Unauthorized Access to Customer Information and Customer Notice

Response programs specify actions that are to be taken when a financial institution suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.[6] A response program is the principal means for a financial institution to protect against unauthorized "use" of customer information that could lead to "substantial harm or inconvenience" to the institution's customer. For example, customer notification is an important tool that enables a customer to take steps to prevent identity theft, such as by arranging to have a fraud alert placed in his or her credit file.

5. A *service provider* is deemed to be a person or entity that maintains, processes, or is otherwise permitted access to customer information through its provision of services directly to the bank.

6. See the information security standards, 12 CFR 208, appendix D-2, section III.C.

The measures enumerated in the information security standards include "response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies."[7] Prompt action by both the institution and the customer following the unauthorized access to customer information is crucial to limiting identity theft. As a result, every financial institution should develop and implement a response program appropriate to its size and complexity and to the nature and scope of its activities. The program should be designed to address incidents of unauthorized access to customer information.

The Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice[8] (the guidance) interprets section 501(b) of the Gramm-Leach-Bliley Act (the GLB Act) and the information security standards.[9] The guidance describes the response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer.

When evaluating the adequacy of an institution's information security program that is required by the information security standards, examiners are to consider whether the institution has developed and implemented a response program equivalent to the guidance. At a minimum, an institution's response program should contain procedures for (1) assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused; (2) notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined later in the guidance; (3) immediately notifying law enforcement in situations involving federal criminal violations requiring immediate attention; (4) taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and (5) notifying customers when warranted.

The guidance does not apply to a financial institution's foreign offices, branches, or affiliates. However, a financial institution subject to the information security standards is responsible for the security of its customer information, whether the information is maintained within or outside of the United States, such as by a service provider located outside of the United States.

The guidance also applies to *customer information,* meaning any record containing "nonpublic personal information" about a financial institution's customer, whether the information is maintained in paper, electronic, or other form, *that is maintained by or on behalf of the institution.*[10] (See the Board's privacy rule, Regulation P, at section 216.3(n)(2) (12 CFR 216.3 (n)(2).) Consequently, the guidance applies only to information that is within the control of the institution and its service providers. The guidance would not apply to information directly disclosed by a customer to a third party, for example, through a fraudulent web site.

The guidance also does not apply to information involving business or commercial accounts. Instead, the guidance applies to nonpublic personal information about a *customer,* as that term is used in the information security standards, namely, a consumer who obtains a financial product or service from a financial institution to be used primarily for personal, family, or household purposes and who has a continuing relationship with the institution.[11]

Response Programs

Financial institutions should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information. For example, financial institutions should place access controls on customer information systems and conduct background

7. See the information security standards, section III.C.1.g.

8. The guidance was jointly issued on March 23, 2005 (effective March 29, 2005), by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

9. See 12 CFR 208, appendix D-2, and 12 CFR 225, appendix F. The Interagency Guidelines Establishing Information Security Standards were formerly known as the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

10. See the information security standards, 12 CFR 208, appendix D-2, section I.C.2.e.

11. See the information security standards, 12 CFR 208, appendix D-2, section I.C.2.d., and the Board's privacy rule (Regulation P), section 216.3(h) (12 CFR 216.3(h)).

checks for employees who are authorized to access customer information.[12] However, every financial institution should also develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems[13] that occur nonetheless. A response program should be a key part of an institution's information security program.[14] The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to customer information in customer information systems maintained by its domestic and foreign service providers. Therefore, consistent with the obligations in the information security standards that relate to these arrangements, and with existing guidance on this topic issued by the agencies,[15] an institution's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the financial institution's customer information, including notification to the institution as soon as possible of any such incident, to enable the institution to expeditiously implement its response program.

Components of a response program. At a minimum, an institution's response program should contain procedures for the following:

- assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused
- notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of *sensitive* customer information, as defined below
- consistent with the Suspicious Activity Report regulations,[16] notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing
- taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence
- notifying customers when warranted

Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's customers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's customers or regulator on its behalf.

Customer Notice

Financial institutions have an affirmative duty to protect their customers' information against unauthorized access or use. Notifying customers of a security incident involving the unauthorized access or use of the customer's information in accordance with the standard set forth below is a key part of that duty. Timely notification of customers is important to managing an institution's reputation risk. Effective notice also may reduce an institution's legal risk, assist in maintaining good customer relations, and enable the institution's customers to take steps to protect themselves against the consequences of identity theft. When customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so.

12. Institutions should also conduct background checks of employees to ensure that the institution does not violate 12 U.S.C. 1829, which prohibits an institution from hiring an individual convicted of certain criminal offenses or who is subject to a prohibition order under 12 U.S.C. 1818(e)(6).

13. Under the information security standards, an institution's *customer information systems* consist of all the methods used to access, collect, store, use, transmit, protect, or dispose of customer information, including the systems maintained by its service providers. See the information security standards, 12 CFR 208, appendix D-2, section I.C.2.f.

14. Reserved footnote.

15. See SR-13-19/CA-13-21, "Guidance on Managing Outsourcing Risk."

16. An institution's obligation to file a SAR is set out in regulations and supervisory guidance. See 12 CFR 208.62 (state member banks); 12 CFR 211.5(k) (Edge and agreement corporations); 12 CFR 211.24(f) (uninsured state branches and agencies of foreign banks); and 12 CFR 225.4(f) (bank holding companies and their nonbank subsidiaries). See the FFIEC BSA/AML Examination Manual and also SR-01-11, "Identity Theft and Pretext Calling."

Standard for providing notice. When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.

Sensitive customer information. Under the information security standards, an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to *sensitive customer information* because this type of information is most likely to be misused, as in the commission of identity theft. For purposes of the guidance, *sensitive customer information* means a customer's name, address, or telephone number, in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as a user name and password or a password and an account number.

Affected customers. If a financial institution, on the basis of its investigation, can determine from its logs or other data precisely which customers' information has been improperly accessed, it may limit notification to those customers for whom the institution determines that misuse of their information has occurred or is reasonably possible. However, there may be situations in which the institution determines that a group of files has been accessed improperly but is unable to identify which specific customers' information has been accessed. If the circumstances of the unauthorized access lead the institution to determine that misuse of the information is reasonably possible, it should notify all customers in the group.

Content of customer notice. Customer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of customer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect the customers' information from further unauthorized access. In addition, it should include a telephone number that customers can call for further information and assistance.[17] The notice also should remind customers of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected identity theft to the institution. The notice should include the following additional items, when appropriate:

- a recommendation that the customer review account statements and immediately report any suspicious activity to the institution
- a description of fraud alerts and an explanation of how the customer may place a fraud alert in the customer's consumer reports to put the customer's creditors on notice that the customer may be a victim of fraud
- a recommendation that the customer periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted
- an explanation of how the customer may obtain a credit report free of charge
- information about the availability of the FTC's online guidance regarding steps a consumer can take to protect against identity theft (The notice should encourage the customer to report any incidents of identity theft to the FTC and should provide the FTC's web site address and toll-free telephone number that customers may use to obtain the identity theft guidance and to report suspected incidents of identity theft.[18]

17. The institution should, therefore, ensure that it has reasonable policies and procedures in place, including trained personnel, to respond appropriately to customer inquiries and requests for assistance.

18. The FTC website for the ID theft brochure and the FTC hotline phone number are www.ftc.gov/bcp/edu/microsites/idtheft/ and 1-877-IDTHEFT. The institution may also refer

Financial institutions are encouraged to notify the nationwide consumer reporting agencies before sending notices to a large number of customers when those notices include contact information for the reporting agencies.

Delivery of customer notice. Customer notice should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it. For example, the institution may choose to contact all affected customers by telephone, by mail, or by electronic mail, in the case of customers for whom it has a valid e-mail address and who have agreed to receive communications electronically.

IDENTITY THEFT RED FLAGS PROGRAM

The federal financial institution regulatory agencies[18a] and the Federal Trade Commission (FTC) have issued joint regulations and guidelines on the *detection, prevention,* and *mitigation* of identity theft in connection with opening of certain accounts or maintaining certain existing accounts in response to the Fair and Accurate Credit Transactions Act of 2003 (The FACT Act).[18b] The regulations require (debit and credit) card issuers to validate notifications of changes of address under certain circumstances. The joint rules also provide guidelines regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy. Financial institutions or creditors[18c] that offer or maintain one or more "covered accounts" must develop and implement a written Identity Theft Prevention Program (Program).[18d] A Program is to be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be tailored to the entity's size, complexity, and the nature and scope of its operations and activities.

The Board's approval of the rule and guidelines was on October 16, 2007. The effective date for the joint final rules and guidelines is January 1, 2008. The mandatory compliance date for the rules is November 1, 2008. See section 222 of the Board's Regulation V—Fair Credit Reporting (12 CFR 222) and 72 *Fed. Reg.* 63718- 63775, November 9, 2007.

This section incorporates certain financial institution safety and soundness provisions of the rule (Regulation V and its guidelines (Appendix J)). See also the October 10, 2008, Federal Reserve Board letter (SR-08-7/CA-08-10) and its interagency attachments.

Risk Assessment

Prior to the development of the Program, a financial institution must initially and then periodically conduct a risk assessment to determine whether it offers or maintains covered accounts. It must take into consideration: (1) the methods it provides to open its accounts, (2) the methods it provides to access accounts, and (3) its previous experiences with identity theft. If the financial institution has covered accounts, it must evaluate its potential vulnerability to identity theft. The institution should also consider whether a reasonably foreseeable risk of identity theft may exist in connection with the accounts it offers or maintains and those that may be opened or accessed remotely, through methods that do not require face-to-face contact, such as through the internet or telephone. Financial institutions that offer or maintain business accounts that have been the target of identity theft should factor those experiences with identity theft into their determination.

If the financial institution determines that it has covered accounts, the risk assessment will

customers to any materials developed pursuant to section 151(b) of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act) (educational materials developed by the FTC to teach the public how to prevent identity theft).

18a. The Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA).

18b. Section 111 of the FACT Act defines "identity theft" as "a fraud committed or attempted using the identifying information of another person."

18c. The term financial institution should be interpreted to mean a "financial institution or creditors" with regard to the Red Flags Program joint regulations and the accompanying interagency guidance.

18d. "Covered accounts" are (1) accounts that a financial institution offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and (2) any other account that the financial institution offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution from identity theft.

enable it to identify which of its accounts the Program must address. If a financial institution initially determines that it does not have covered accounts, it must periodically reassess whether it must develop and implement a Program in light of changes in the accounts that it offers or maintains.

Elements of the Program

The elements of the actual Program will vary depending on the size and complexity of the financial institution. A financial institution that determines that it is required to establish and maintain an Identity Theft Prevention Program must (1) identify relevant Red Flags for its covered accounts, (2) detect and respond to the Red Flags that have been incorporated into its Program, and (3) respond appropriately to the detected Red Flags. The Red Flags are patterns, practices, or specific activities that indicate the possible existence of identity theft or the potential to lead to identity theft. A financial institution must ensure that its Program is updated periodically to address the changing risks associated with its customers and their accounts and to the safety and soundness of the financial institution from identity theft.

Guidelines

Each financial institution that is required to implement a written Program must consider the Guidelines for Identity Theft Detection, Prevention, and Mitigation's in Appendix J (12 CFR 222, Appendix J of the rule) (the Guidelines) and include those guidelines that are appropriate in its Program. Section I of the Guidelines, "The Program," discusses a Program's design that may include, as appropriate, existing policies, procedures, and arrangements that control foreseeable risks to the institution's customers or to the safety and soundness of the financial institution from identity theft.

Identification of Red Flags

A financial institution should incorporate relevant Red Flags into the Program from sources such as (1) incidents of identity theft that it has experienced, (2) methods of identity theft that have been identified as reflecting changes in identity theft risks, and (3) applicable supervisory guidance.

Categories of Red Flags

Section II of the Guidelines, "Categories of Red Flags," provides some guidance in identifying relevant Red Flags. A financial institution should include, as appropriate,[18e]

- alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
- the presentation of suspicious documents
- the presentation of suspicious personal identifying information, such as a suspicious address change
- the unusual use of, or other suspicious activity related to, a covered account
- a notice received from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution

The above categories do not represent a comprehensive list of all types of Red Flags that may indicate the possibility of identity theft. Institutions must also consider specific business lines and any previous exposures to identity theft. No specific Red Flag is mandatory for all financial institutions. Rather, the Program should follow the risk-based, nonprescriptive approach regarding the identification of Red Flags.

Detect the Program's Red Flags

In accordance with Section III of the Guidelines, each financial institution's Program should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts. A financial institution is required to detect, prevent, and mitigate identity theft in connection with such accounts. The policies and procedures regarding opening a covered account subject to the Program should explain how an institution could identify information about, and verify the identity of, a person

18e. Examples of Red Flags from each of these categories are appended as supplement A to appendix J.

opening an account.[18f] In the case of existing covered accounts, institutions could authenticate customers, monitor transactions, and verify the validity of change of address requests.

Respond Appropriately to any Detected Red Flags

A financial institution should consider precursors to identity theft to stop identity theft before it occurs. Section IV of the Guidelines, "Prevention and Mitigation," states that an institution's procedures should provide for appropriate responses to Red Flags that it has detected that are commensurate with the degree of risk posed. When determining an appropriate response, the institution should consider aggravating factors that may heighten its risk of identity theft. Such factors may include (1) a data security incident that results in unauthorized disclosures of nonpublic personal information (NPPI), (2) records the financial institution holds or that are held by another creditor or third party, or (3) notice that the institution's customer has provided information related to its covered account to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following: (1) monitoring a covered account for evidence of identity theft; (2) contacting the customer; (3) changing any passwords, security codes, or other security devices that permit access to a secured account; (4) reopening a covered account with a new account number; (5) not opening a new covered account; (6) closing an existing covered account; (7) not attempting to collect on a covered account or not selling a covered account to a debt collector; (8) notifying law enforcement; or (9) determining that no response is warranted under the particular circumstances.

Periodically Updating the Program's Relevant Red Flags

Section V of the Guidelines, "Updating the Program," states that a financial institution should periodically update its Program (including its relevant Red Flags) to reflect any changes in risks to its customers or to the safety and soundness of the institution from identity theft, based on (but not limited to) factors such as

- the experiences of the financial institution with identity theft;
- changes in methods of identity theft;
- changes in methods to detect, prevent, and mitigate identity theft;
- changes in the types of accounts that the financial institution offers or maintains; and
- changes in the financial institution's structure, including its mergers, acquisitions, joint ventures, and any business arrangements, such as alliances and service provider arrangements.

Administration of Program

A financial institution that is required to implement a Program must provide for the continued oversight and administration of its Program. The following are the steps that are needed in the administration of a Red Flags Program:

1. *Obtain approval from either the institution's board of directors or any appropriate committee of the board of directors of the initial written Program;*
2. *Involve either the board of directors, a designated committee of the board of directors, or a designated senior-management-level employee in the oversight, development, implementation, and administration of the Program.* This includes
   - assigning specific responsibility for the Program's implementation,
   - reviewing reports prepared by staff regarding the institution's compliance (the reports should be prepared at least annually), and
   - reviewing material changes to the Program as necessary to address changing identity theft risks.
3. *Train staff.* The financial institution must train relevant staff to effectively implement and monitor the Program. Training should be provided as changes are made to the financial institution's Program based on its periodic risk assessment.
4. *Exercise appropriate and effective oversight of service provider arrangements.* Section VI of the Guidelines, "Methods for Administering the Program," indicates a financial institution is ultimately responsible for complying with the rules and guidelines for out-

18f. 31 U.S.C. 5318(l) (31 CFR 103.121).

sourcing an activity to a third-party service provider. Whenever a financial institution engages a service provider to perform an activity in connection with one or more covered accounts, the institution should ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. With regard to the institution's oversight of its Program, periodic reports from service providers are to be issued on the Program's development, implementation, and administration.

IT EXAMINATION FREQUENCY AND SCOPE

All safety-and-soundness examinations (or examination cycles) of banking organizations conducted by the Federal Reserve should include an assessment and evaluation of IT risks and risk management. The scope of the IT assessment should generally be sufficient to assign a composite rating under the Uniform Rating System for Information Technology (URSIT). URSIT component ratings may be updated at the examiner's discretion, based on the scope of the assessment. The scope would normally be based on factors such as—

- implementation of new systems or technologies since the last examination;
- significant changes in operations, such as mergers or systems conversions;
- new or modified outsourcing relationships for critical operations;
- targeted examinations of business lines whose internal controls or risk-management systems depend heavily on IT; and
- other potential problems or concerns that may have arisen since the last examination or the need to follow up on previous examination or audit issues.

Institutions that outsource core processing functions, although not traditionally subject to IT examinations, are exposed to IT-related risks. For these institutions, some or all components of the URSIT rating may not be meaningful. In these cases, the assessment of IT activities may be incorporated directly into the safety-and soundness rating for the institution, rather than through the assignment of an URSIT rating. The scope of the IT assessment for such institutions should evaluate the adequacy of the institution's oversight of service providers for critical processing activities and should incorporate the results of any relevant supervisory reviews of these service providers. The assessment should also include reviews of any significant in-house activities, such as management information systems and local networks, and the implementation of new technologies, such as Internet banking. As noted above, the assessment of IT should be reflected in the overall safety-and- soundness examination report and in the appropriate components of the safety-and-soundness examination rating assigned to the institution, as well as in the associated risk-profile analysis. (See SR-00-3.)

Targeted IT examinations may be conducted more frequently, if deemed necessary, by the Reserve Bank. A composite URSIT rating should be assigned for targeted reviews when possible. In addition, institutions for which supervisory concerns have been raised (normally those rated URSIT 3, 4, or 5) should be subject to more frequent IT reviews, until such time as the Reserve Bank is satisfied that the deficiencies have been corrected.

RISK ELEMENTS

To provide a common terminology and consistent approach for evaluating the adequacy of an organization's IT, five IT elements are defined below. These elements may be used to evaluate the IT processes at the functional business level or for the organization as a whole and to determine the impact on the business risks outlined in SR-95-51 and SR-16-11, as well as their impact on the IT rating (URSIT) discussed below. (See SR-98-9.)

1. *Management processes.* Management processes encompass planning, investment, development, execution, and staffing of IT from a corporate-wide and business-specific perspective. Management processes over IT are effective when they are adequately and appropriately aligned with and support the organization's mission and business objectives. Management processes include strategic planning; budgeting; management and reporting hierarchy; management succession; and a regular, independent review function.

Examiners should determine if the IT strategy for the business activity or organization is consistent with the organization's mission and business objectives and whether the IT function has effective management processes to execute that strategy.

2. *Architecture.* Architecture refers to the underlying design of an automated information system and its individual components. The underlying design encompasses both physical and logical architecture, including operating environments, as well as the organization of data. The individual components refer to network communications, hardware, and software, which includes operating systems, communications software, database-management systems, programming languages, and desktop software. Effective architecture meets current and long-term organizational objectives, addresses capacity requirements to ensure that systems allow users to easily enter data at both normal and peak processing times, and provides satisfactory solutions to problems that arise when information is stored and processed in two or more systems that cannot be connected electronically. When assessing the adequacy of IT architecture, examiners should consider the ability of the current infrastructure to meet operating objectives, including the effective integration of systems and sources of data.
3. *Integrity.* Integrity refers to the reliability, accuracy, and completeness of information delivered to the end-user. Integrity risk could arise from insufficient controls over systems or data, which could adversely affect critical financial and customer information. Examiners should review and consider whether the organization relies on information system audits or independent reviews of applications to ensure the integrity of its systems. Examiners should review the reliability, accuracy, and completeness of information delivered in key business lines.
4. *Security.* Security risk is the risk of unauthorized disclosure or destruction of critical or sensitive information. To mitigate this risk, physical access and logical controls are generally provided to achieve a level of protection commensurate with the value of the information. Security risk is managed effectively when controls prevent unauthorized access, modification, destruction, or disclosure of sensitive information during creation, transmission, processing, maintenance, or storage. Examiners should ensure that operating procedures and controls are commensurate with the potential for and risks associated with security breaches, which may be either physical or electronic, inadvertent or intentional, internal or external.
5. *Availability.* Availability refers to the timely delivery of information and processes to end-users in support of business and decision-making processes and customer services. In assessing the management of availability risk, examiners should consider the capability of IT functions to provide information to the end-users from either primary or secondary sources, as well as consider the ability of back-up systems, as presented in contingency plans, to mitigate business disruption. Contingency plans should set out a process for an organization to restore or replace its information-processing resources; reconstruct its information assets; and resume its business activity from disruption caused by human error or intervention, natural disaster, or infrastructure failure (including loss of utilities and communication lines and the operational failure of hardware, software, and network communications).

UNIFORM RATING SYSTEM FOR INFORMATION TECHNOLOGY

The Uniform Rating System for Information Technology (URSIT) is an interagency examination rating system adopted by the Federal Financial Institutions Examination Council (FFIEC) agencies to evaluate the IT activities of financial institutions. The rating system includes component- and composite-rating descriptions and the explicit identification of risks and assessment factors that examiners consider inassigning component ratings. This rating system helps examiners assess risk and compile examination findings. However, the rating system should not drive the scope of an examination. In particular, not all assessment factors or component-rating areas are required to be assessed at each examination. Examiners should use the rating system to help evaluate the entity's overall risk exposure and risk-management performance and to determine the degree of supervisory attention believed neces-

sary to ensure that weaknesses are addressed and that risk is properly managed. (See SR-99-8.)

The URSIT rating framework is based on a risk evaluation of four general areas: audit, management, development and acquisition, and support and delivery. These components are used to assess the overall IT functions within an organization and arrive at a composite URSIT rating. Examiners evaluate the areas identified within each component to assess the institution's ability to identify, measure, monitor, and control IT risks.

In adopting the URSIT rating system, the FFIEC recognized that management practices vary considerably among financial institutions depending on their size and sophistication, the nature and complexity of their business activities, and their risk profile. For less complex information systems environments, detailed or highly formalized systems and controls are not required to receive the higher composite and component ratings.

URSIT Composite-Rating Definitions

Financial institutions rated URSIT composite 1 exhibit strong performance in every respect and generally have components rated 1 or 2. Weaknesses in IT functions are minor and are easily corrected during the normal course of business. Risk-management processes provide a comprehensive program to identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are well defined and fully integrated throughout the organization. This allows management to quickly adapt to the changing market, business, and technology needs of the entity. Management identifies weaknesses promptly and takes appropriate corrective action to resolve audit and regulatory concerns.

Financial institutions rated URSIT composite 2 exhibit safe and sound performance but may demonstrate modest weaknesses in operating performance, monitoring, management processes, or system development. Generally, senior management corrects weaknesses in the normal course of business. Risk-management processes adequately identify and monitor risk relative to the size, complexity, and risk profile of the entity. Strategic plans are defined but may require clarification, better coordination, or improved communication throughout the organization. As a result, management anticipates, but responds less quickly to changes in the market, business, and technological needs of the entity. Management normally identifies weaknesses and takes appropriate corrective action. However, greater reliance is placed on audit and regulatory intervention to identify and resolve concerns. While internal control weaknesses may exist, there are no significant supervisory concerns. As a result, supervisory action is informal and limited.

Financial institutions rated URSIT composite 3 exhibit some degree of supervisory concern due to a combination of weaknesses that may range from moderate to severe. If weaknesses persist, further deterioration in the condition and performance of the institution is likely. Risk-management processes may not effectively identify risks and may not be appropriate for the size, complexity, or risk profile of the entity. Strategic plans are vaguely defined and may not provide adequate direction for IT initiatives. As a result, management often has difficulty responding to changes in the business, market, and technological needs of the entity. Self-assessment practices are weak and generally reactive to audit and regulatory exceptions. Repeat concerns may exist, indicating that management may lack the ability or willingness to resolve concerns. While financial or operational failure is unlikely, increased supervision is necessary. Formal or informal supervisory action may be necessary to secure corrective action.

Financial institutions rated URSIT composite 4 operate in an unsafe and unsound environment that may impair the future viability of the entity. Operating weaknesses are indicative of serious managerial deficiencies. Risk-management processes inadequately identify and monitor risk, and practices are not appropriate given the size, complexity, and risk profile of the entity. Strategic plans are poorly defined and not coordinated or communicated throughout the organization. As a result, management and the board are not committed to, or may be incapable of, ensuring that technological needs are met. Management does not perform self-assessments and demonstrates an inability or unwillingness to correct audit and regulatory concerns. Failure of the financial institution may be likely unless IT problems are remedied. Close supervisory attention is necessary and, in most cases, formal enforcement action is warranted.

Financial institutions rated URSIT composite 5 exhibit critically deficient operating performance and are in need of immediate remedial action. Operational problems and serious weak-

nesses may exist throughout the organization. Risk-management processes are severely deficient and provide management little or no perception of risk relative to the size, complexity, and risk profile of the entity. Strategic plans do not exist or are ineffective, and management and the board provide little or no direction for IT initiatives. As a result, management is unaware of or inattentive to the technological needs of the entity. Management is unwilling or incapable of correcting audit and regulatory concerns. Ongoing supervisory attention is necessary.

URSIT Component Ratings

Audit

Financial institutions and service providers are expected to provide independent assessments of their exposure to risks and of the quality of internal controls associated with the acquisition, implementation, and use of IT. Audit practices should address the IT risk exposures throughout the institution and the exposures of its service provider(s) in the areas of user and data center operations, client/server architecture, local and wide area networks, telecommunications, information security, electronic data interchange, systems development, and contingency planning. This rating should reflect the adequacy of the organization's overall IT audit program, including the internal and external auditor's abilities to detect and report significant risks to management and the board of directors on a timely basis. It should also reflect the internal and external auditor's capability to promote a safe, sound, and effective operation. The performance of an audit is rated based on an assessment of factors such as—

- the level of independence maintained by audit and the quality of the oversight and support provided by the board of directors and management;
- the adequacy of audit's risk-analysis methodology used to prioritize the allocation of audit resources and to formulate the audit schedule;
- the scope, frequency, accuracy, and timeliness of internal and external audit reports;
- the extent of audit participation in application development, acquisition, and testing, to ensure the effectiveness of internal controls and audit trails;
- the adequacy of the overall audit plan in providing appropriate coverage of IT risks;
- the auditor's adherence to codes of ethics and professional audit standards;
- the qualifications of the auditor, staff succession, and continued development through training;
- the existence of timely and formal follow-up and reporting on management's resolution of identified problems or weaknesses; and
- the quality and effectiveness of internal and external audit activity as it relates to IT controls.

A rating of 1 indicates strong audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or its audit committee in a thorough and timely manner. Outstanding audit issues are monitored until resolved. Risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities with appropriate scope and frequency. Audit work is performed in accordance with professional auditing standards, and report content is timely, constructive, accurate, and complete. Because audit is strong, examiners may place substantial reliance on audit results.

A rating of 2 indicates satisfactory audit performance. Audit independently identifies and reports weaknesses and risks to the board of directors or audit committee, but reports may be less timely. Significant outstanding audit issues are monitored until resolved. Risk analysis ensures that audit plans address all significant IT operations, procurement, and development activities; however, minor concerns may be noted with the scope or frequency. Audit work is performed in accordance with professional auditing standards; however, minor or infrequent problems may arise with the timeliness, completeness, and accuracy of reports. Because audit is satisfactory, examiners may rely on audit results but because minor concerns exist, examiners may need to expand verification procedures in certain situations.

A rating of 3 indicates less-than-satisfactory audit performance. Audit identifies and reports weaknesses and risks; however, independence may be compromised and reports presented to the board or audit committee may be less than satisfactory in content and timeliness. Outstanding audit issues may not be adequately moni-

tored. Risk analysis is less than satisfactory. As a result, the audit plan may not provide sufficient audit scope or frequency for IT operations, procurement, and development activities. Audit work is generally performed in accordance with professional auditing standards; however, occasional problems may be noted with the timeliness, completeness, or accuracy of reports. Because audit is less than satisfactory, examiners must use caution if they rely on the audit results.

A rating of 4 indicates deficient audit performance. Audit may identify weaknesses and risks, but it may not independently report to the board or audit committee, and report content may be inadequate. Outstanding audit issues may not be adequately monitored and resolved. Risk analysis is deficient. As a result, the audit plan does not provide adequate audit scope or frequency for IT operations, procurement, and development activities. Audit work is often inconsistent with professional auditing standards, and the timeliness, accuracy, and completeness of reports is unacceptable. Because audit is deficient, examiners cannot rely on audit results.

A rating of 5 indicates critically deficient audit performance. If an audit function exists, it lacks sufficient independence and, as a result, does not identify and report weaknesses or risks to the board or audit committee. Outstanding audit issues are not tracked and no follow-up is performed to monitor their resolution. Risk analysis is critically deficient. As a result, the audit plan is ineffective and provides inappropriate audit scope and frequency for IT operations, procurement, and development activities. Audit work is not performed in accordance with professional auditing standards and major deficiencies are noted regarding the timeliness, accuracy, and completeness of audit reports. Because audit is critically deficient, examiners cannot rely on audit results.

Management

The management rating reflects the abilities of the board and management as they apply to all aspects of IT acquisition, development, and operations. Management practices may need to address some or all of the following IT-related risks: strategic planning, quality assurance, project management, risk assessment, infrastructure and architecture, end-user computing, contract administration of third-party service providers, organization and human resources, and regulatory and legal compliance. Generally, directors need not be actively involved in day-to-day operations; however, they must provide clear guidance regarding acceptable risk-exposure levels and ensure that appropriate policies, procedures, and practices have been established. Sound management practices are demonstrated through active oversight by the board of directors and management, competent personnel, sound IT plans, adequate policies and standards, an effective control environment, and risk monitoring. The management rating should reflect the board's and management's ability as it applies to all aspects of IT operations. The performance of management and the quality of risk management are rated based on an assessment of factors such as—

- the level and quality of oversight and support of the IT activities by the board of directors and management;
- the ability of management to plan for and initiate new activities or products in response to information needs and to address risks that may arise from changing business conditions;
- the ability of management to provide information reports necessary for informed planning and decision making in an effective and efficient manner;
- the adequacy of, and conformance with, internal policies and controls addressing the IT operations and risks of significant business activities;
- the effectiveness of risk-monitoring systems;
- the timeliness of corrective action for reported and known problems;
- the level of awareness of and compliance with laws and regulations;
- the level of planning for management succession;
- the ability of management to monitor the services delivered and to measure the organization's progress toward identified goals effectively and efficiently;
- the adequacy of contracts and management's ability to monitor relationships with third-party servicers;
- the adequacy of strategic planning and risk-management practices to identify, measure, monitor, and control risks, including management's ability to perform self-assessments; and

- the ability of management to identify, measure, monitor, and control risks and to address emerging IT needs and solutions.

A rating of 1 indicates strong performance by management and the board. Effective risk-management practices are in place to guide IT activities, and risks are consistently and effectively identified, measured, controlled, and monitored. Management immediately resolves audit and regulatory concerns to ensure sound operations. Written technology plans, policies and procedures, and standards are thorough and properly reflect the complexity of the IT environment. They have been formally adopted, communicated, and enforced throughout the organization. IT systems provide accurate, timely reports to management. These reports serve as the basis for major decisions and as an effective performance-monitoring tool. Outsourcing arrangements are based on comprehensive planning; routine management supervision sustains an appropriate level of control over vendor contracts, performance, and services provided. Management and the board have demonstrated the ability to promptly and successfully address existing IT problems and potential risks.

A rating of 2 indicates satisfactory performance by management and the board. Adequate risk-management practices are in place and guide IT activities. Significant IT risks are identified, measured, monitored, and controlled; however, risk-management processes may be less structured or inconsistently applied and modest weaknesses exist. Management routinely resolves audit and regulatory concerns to ensure effective and sound operations; however, corrective actions may not always be implemented in a timely manner. Technology plans, policies and procedures, and standards are adequate and formally adopted. However, minor weaknesses may exist in management's ability to communicate and enforce them throughout the organization. IT systems provide quality reports to management which serve as a basis for major decisions and a tool for performance planning and monitoring. Isolated or temporary problems with timeliness, accuracy, or consistency of reports may exist. Outsourcing arrangements are adequately planned and controlled by management, and they provide for a general understanding of vendor contracts, performance standards, and services provided. Management and the board have demonstrated the ability to address existing IT problems and risks successfully.

A rating of 3 indicates less-than-satisfactory performance by management and the board. Risk-management practices may be weak and offer limited guidance for IT activities. Most IT risks are generally identified; however, processes to measure and monitor risk may be flawed. As a result, management's ability to control risk is less than satisfactory. Regulatory and audit concerns may be addressed, but time frames are often excessive and the corrective action taken may be inappropriate. Management may be unwilling or incapable of addressing deficiencies. Technology plans, policies and procedures, and standards exist but may be incomplete. They may not be formally adopted, effectively communicated, or enforced throughout the organization. IT systems provide requested reports to management, but periodic problems with accuracy, consistency, and timeliness lessen the reliability and usefulness of reports and may adversely affect decision making and performance monitoring. Outsourcing arrangements may be entered into without thorough planning. Management may provide only cursory supervision that limits their understanding of vendor contracts, performance standards, and services provided. Management and the board may not be capable of addressing existing IT problems and risks, which is evidenced by untimely corrective actions for outstanding IT problems.

A rating of 4 indicates deficient performance by management and the board. Risk-management practices are inadequate and do not provide sufficient guidance for IT activities. Critical IT risks are not properly identified, and processes to measure and monitor risks are deficient. As a result, management may not be aware of and is unable to control risks. Management may be unwilling or incapable of addressing audit and regulatory deficiencies in an effective and timely manner. Technology plans, policies and procedures, and standards are inadequate and have not been formally adopted or effectively communicated throughout the organization, and management does not effectively enforce them. IT systems do not routinely provide management with accurate, consistent, and reliable reports, thus contributing to ineffective performance monitoring or flawed decision making. Outsourcing arrangements may be entered into without planning or analysis, and management may provide little or no supervision of vendor contracts, performance standards, or services pro-

vided. Management and the board are unable to address existing IT problems and risks, as evidenced by ineffective actions and long-standing IT weaknesses. Strengthening of management and its processes is necessary.

A rating of 5 indicates critically deficient performance by management and the board. Risk-management practices are severely flawed and provide inadequate guidance for IT activities. Critical IT risks are not identified, and processes to measure and monitor risks do not exist or are not effective. Management's inability to control risk may threaten the continued viability of the institution. Management is unable or unwilling to correct audit- and regulatory-identified deficiencies, and immediate action by the board is required to preserve the viability of the institution. If they exist, technology plans, policies and procedures, and standards are critically deficient. Because of systemic problems, IT systems do not produce management reports that are accurate, timely, or relevant. Outsourcing arrangements may have been entered into without management planning or analysis, resulting in significant losses to the financial institution or ineffective vendor services.

Development and Acquisition

The rating of development and acquisition reflects an organization's ability to identify, acquire, install, and maintain appropriate IT resources. Management practices may need to address all or parts of the business process for implementing any kind of change to the hardware or software used. These business processes include an institution's purchase of hardware or software, development and programming performed by the institution, purchase of services from independent vendors or affiliated data centers, or a combination of these activities. The business process is defined as all phases taken to implement a change, including researching alternatives available, choosing an appropriate option for the organization as a whole, and converting to the new system or integrating the new system with existing systems. This rating reflects the adequacy of the institution's systems-development methodology and related risk-management practices for acquisition and deployment of IT. This rating also reflects the board and management's ability to enhance and replace IT prudently in a controlled environment. The performance of systems development and acquisition and related risk-management practice is rated based on an assessment of factors such as—

- the level and quality of oversight and support of systems-development and acquisition activities by senior management and the board of directors;
- the adequacy of the organizational and management structures to establish accountability and responsibility for IT systems and technology initiatives;
- the volume, nature, and extent of risk exposure to the financial institution in the area of systems development and acquisition;
- the adequacy of the institution's Systems Development Life Cycle (SDLC) and programming standards;
- the quality of project-management programs and practices that are followed by developers, operators, executive management or owners, independent vendors or affiliated servicers, and end-users;
- the independence of the quality-assurance function and the adequacy of controls over program changes;
- the quality and thoroughness of system documentation;
- the integrity and security of the network, system, and application software;
- the development of IT solutions that meet the needs of end-users; and
- the extent of end-user involvement in the system-development process.

A rating of 1 indicates strong systems-development, acquisition, implementation, and change-management performance. Management and the board routinely demonstrate successfully the ability to identify and implement appropriate IT solutions while effectively managing risk. Project-management techniques and the SDLC are fully effective and supported by written policies, procedures, and project controls that consistently result in timely and efficient project completion. An independent quality-assurance function provides strong controls over testing and program-change management. Technology solutions consistently meet end-user needs. No significant weaknesses or problems exist.

A rating of 2 indicates satisfactory systems-development, acquisition, implementation, and change-management performance. Management and the board frequently demonstrate the ability

to identify and implement appropriate IT solutions while managing risk. Project management and the SDLC are generally effective; however, weaknesses may exist that result in minor project delays or cost overruns. An independent quality-assurance function provides adequate supervision of testing and program-change management, but minor weaknesses may exist. Technology solutions meet end-user needs. However, minor enhancements may be necessary to meet original user expectations. Weaknesses may exist; however, they are not significant and are easily corrected in the normal course of business.

A rating of 3 indicates less-than-satisfactory systems-development, acquisition, implementation, and change-management performance. Management and the board may often be unsuccessful in identifying and implementing appropriate IT solutions; therefore, unwarranted risk exposure may exist. Project-management techniques and the SDLC are weak and may result in frequent project delays, backlogs, or significant cost overruns. The quality-assurance function may not be independent of the programming function, which may have an adverse impact on the integrity of testing and program-change management. Technology solutions generally meet end-user needs but often require an inordinate level of change after implementation. Because of weaknesses, significant problems may arise that could result in disruption to operations or significant losses.

A rating of 4 indicates deficient systems-development, acquisition, implementation, and change-management performance. Management and the board may be unable to identify and implement appropriate IT solutions and do not effectively manage risk. Project-management techniques and the SDLC are ineffective and may result in severe project delays and cost overruns. The quality-assurance function is not fully effective and may not provide independent or comprehensive review of testing controls or program-change management. Technology solutions may not meet the critical needs of the organization. Problems and significant risks exist that require immediate action by the board and management to preserve the soundness of the institution.

A rating of 5 indicates critically deficient systems-development, acquisition, implementation, and change-management performance. Management and the board appear to be incapable of identifying and implementing appropriate IT solutions. If they exist, project-management techniques and the SDLC are critically deficient and provide little or no direction for development of systems or technology projects. The quality-assurance function is severely deficient or not present, and unidentified problems in testing and program-change management have caused significant IT risks. Technology solutions do not meet the needs of the organization. Serious problems and significant risks exist, which raise concern for the financial institution's ongoing viability.

Support and Delivery

The rating of support and delivery reflects an organization's ability to provide technology services in a secure environment. It reflects not only the condition of IT operations but also factors such as reliability, security, and integrity, which may affect the quality of the information-delivery system. The factors include user support and training, as well as the ability to manage problems and incidents, operations, system performance, capacity planning, and facility and data management. Risk-management practices should promote effective, safe, and sound IT operations that ensure the continuity of operations and the reliability and availability of data. The scope of this component rating includes operational risks throughout the organization. The rating of IT support and delivery is based on a review and assessment of requirements such as—

- the ability to provide a level of service that meets the requirements of the business;
- the adequacy of security policies, procedures, and practices in all units and at all levels of the financial institution;
- the adequacy of data controls over preparation, input, processing, and output;
- the adequacy of corporate contingency planning and business resumption for data centers, networks, and business units;
- the quality of processes or programs that monitor capacity and performance;
- the adequacy of controls and the ability to monitor controls at service providers;
- the quality of assistance provided to users, including the ability to handle problems;
- the adequacy of operating policies, procedures, and manuals;
- the quality of physical and electronic security,

including the privacy of data; and
- the adequacy of firewall architectures and the security of connections with public networks.

A rating of 1 indicates strong IT support and delivery performance. The organization provides technology services that are reliable and consistent. Service levels adhere to well-defined service-level agreements and routinely meet or exceed business requirements. A comprehensive corporate contingency and business-resumption plan is in place. Annual contingency-plan testing and updating is performed, and critical systems and applications are recovered within acceptable time frames. A formal written data-security policy and awareness program is communicated and enforced throughout the organization. The logical and physical security for all IT platforms is closely monitored, and security incidents and weaknesses are identified and quickly corrected. Relationships with third-party service providers are closely monitored. IT operations are highly reliable, and risk exposure is successfully identified and controlled.

A rating of 2 indicates satisfactory IT support and delivery performance. The organization provides technology services that are generally reliable and consistent; however, minor discrepancies in service levels may occur. Service performance adheres to service agreements and meets business requirements. A corporate contingency and business-resumption plan is in place, but minor enhancements may be necessary. Annual plan testing and updating is performed, and minor problems may occur when recovering systems or applications. A written data-security policy is in place but may require improvement to ensure its adequacy. The policy is generally enforced and communicated throughout the organization, for example, through a security-awareness program. The logical and physical security for critical IT platforms is satisfactory. Systems are monitored, and security incidents and weaknesses are identified and resolved within reasonable time frames. Relationships with third-party service providers are monitored. Critical IT operations are reliable and risk exposure is reasonably identified and controlled.

A rating of 3 indicates that the performance of IT support and delivery is less than satisfactory and needs improvement. The organization provides technology services that may not be reliable or consistent. As a result, service levels periodically do not adhere to service-level agreements or meet business requirements. A corporate contingency and business-resumption plan is in place but may not be considered comprehensive. The plan is periodically tested; however, the recovery of critical systems and applications is frequently unsuccessful. A data-security policy exists; however, it may not be strictly enforced or communicated throughout the organization. The logical and physical security for critical IT platforms is less than satisfactory. Systems are monitored; however, security incidents and weaknesses may not be resolved in a timely manner. Relationships with third-party service providers may not be adequately monitored. IT operations are not acceptable, and unwarranted risk exposures exist. If not corrected, weaknesses could cause performance degradation or disruption to operations.

A rating of 4 indicates deficient IT support and delivery performance. The organization provides technology services that are unreliable and inconsistent. Service-level agreements are poorly defined and service performance usually fails to meet business requirements. A corporate contingency and business-resumption plan may exist, but its content is critically deficient. If contingency testing is performed, management is typically unable to recover critical systems and applications. A data-security policy may not exist. As a result, serious supervisory concerns over security and the integrity of data exist. The logical and physical security for critical IT platforms is deficient. Systems may be monitored, but security incidents and weaknesses are not successfully identified or resolved. Relationships with third-party service providers are not monitored. IT operations are not reliable and significant risk exposure exists. Degradation in performance is evident and frequent disruption in operations has occurred.

A rating of 5 indicates critically deficient IT support and delivery performance. The organization provides technology services that are not reliable or consistent. Service-level agreements do not exist, and service performance does not meet business requirements. A corporate contingency and business-resumption plan does not exist. Contingency testing is not performed, and management has not demonstrated the ability to recover critical systems and applications. A data-security policy does not exist, and a serious threat to the organization's security and data integrity exists. The logical and physical security for critical IT platforms is inadequate, and

management does not monitor systems for security incidents and weaknesses. Relationships with third-party service providers are not monitored, and the viability of a service provider may be in jeopardy. IT operations are severely deficient, and the seriousness of weaknesses could cause failure of the financial institution if not addressed.

OUTSOURCING INFORMATION TECHNOLOGY

Banking organizations are increasingly relying on services provided by other entities to support a range of banking operations. Outsourcing of information- and transaction-processing activities, either to affiliated institutions or third-party service providers, may help banking organizations manage data processing and related personnel costs, improve services, and obtain expertise not available internally. At the same time, the reduced operational control over outsourced activities may expose an institution to additional risks. The federal banking agencies have established procedures to examine and evaluate the adequacy of institutions' controls over service providers, which can be found in the FFIEC's *IT Handbook* and related guidance. Additional information on specific areas is provided later in this section.

In the development of the examination scope and risk profile, examiners should determine which information- and transaction-processing activities critical to the institution's core operations are outsourced. During the on-site examination, the adequacy of the institution's risk management for these critical service providers should be assessed and evaluated. The overall assessment should be reflected in the relevant components of the URSIT examination rating or the Uniform Financial Institution Rating System, if an information-systems rating is not assigned.

Outsourcing Risks

The outsourcing of information and transaction processing involves operational risks that are similar to those that arise when the functions are performed internally, such as threats to the availability of systems used to support customer transactions, the integrity or security of customer account information, or the integrity of risk-management information systems. Under outsourcing arrangements, however, the risk-management measures commonly used to address these risks, such as internal controls and procedures, are generally under the direct operational control of the service provider. Nevertheless, the serviced institution would bear the associated risk of financial loss, reputational damage, or other adverse consequences.

Some outsourcing arrangements also involve direct financial risks to the serviced institution. For example, in some transaction-processing activities, a service provider has the ability to process transactions that result in extensions of credit on behalf of the serviced institution.[19] A service provider may also collect or disburse funds, exposing the institution to liquidity and credit risks if the service provider fails to perform as expected.

Risk Management

The Federal Reserve expects institutions to ensure that controls over outsourced information- and transaction-processing activities are equivalent to those that would be implemented if the activity were conducted internally. The institution's board of directors and senior management should understand the key risks associated with the use of service providers for its critical operations, commensurate with the scope and risks of the outsourced activity and its importance to the institution's business. They should ensure that an appropriate oversight program is in place to monitor each service provider's controls, condition, and performance. The following eight areas should be included in this process:

1. *Risk assessment.* Before entering into an outsourcing arrangement, the institution should assess the key risks that may arise and options for controlling these risks. Factors influencing the risk assessment could include how critical the outsourced function is to the institution; the nature of activities to be performed by the service provider, including handling funds or implementing credit deci-

19. For example, an institution may authorize a service provider to originate payments, such as ACH credit transfers, on behalf of customers. The institution is required by law or contract to honor these types of transactions.

sions; the availability of alternative service providers for the particular function; insurance coverage available for particular risks; and the cost and time required to switch service providers if problems arise.

2. *Selection of service provider.* In selecting a service provider for critical information- or transaction-processing functions, an institution should perform sufficient due diligence to satisfy itself of the service provider's competence and stability, both financially and operationally, to provide the expected services and meet any related commitments.[20]
3. *Contracts.* The written contract between the institution and the service provider should clearly specify, at a level of detail commensurate with the scope and risks of the outsourced activity, all relevant terms, conditions, responsibilities, and liabilities of both parties. These would normally include terms such as—
   - required service levels, performance standards, and penalties;
   - internal controls, insurance, disaster-recovery capabilities, and other risk-management measures maintained by the service provider;
   - data and system ownership and access;
   - liability for delayed or erroneous transactions and other potential risks;
   - provisions for the institution to require and have access to internal or external audits or other reviews of the service provider's operations and financial condition;
   - compliance with any applicable regulatory requirements and access to information and operations by the institution's supervisory authorities; and
   - provisions for handling disputes, contract changes, and contract termination.

   Terms and conditions should be assessed by the institution to ensure that they are appropriate for the particular service being provided and result in an acceptable level of risk to the institution.[21] Contracts for outsourcing of critical functions should be reviewed by the institution's legal counsel.
4. *Policies, procedures, and control.* The service provider should implement internal control policies and procedures, data-security and contingency capabilities, and other operational controls analogous to those that the institution would use if it performed the activity internally. Appropriate controls should be placed on transactions processed or funds handled by the service provider on behalf of the institution. The service provider's policies and procedures should be reviewed by client institutions.
5. *Ongoing monitoring.* The institution should review the operational and financial performance of critical service providers on an ongoing basis to ensure that the service provider is meeting and can continue to meet the terms of the arrangement. The institution's staff should have sufficient training and expertise to review the service provider's performance and risk controls.
6. *Information access.* The institution must ensure that it has complete and immediate access to information that is critical to its operations and that is maintained or processed by a service provider. Records maintained at the institution must be adequate to enable examiners to review its operations fully and effectively, even if a function is outsourced.
7. *Audit.* The institution's audit function should review the oversight of critical service providers. Audits of the outsourced function should be conducted according to a scope and frequency appropriate for the particular function. Serviced institutions should conduct audits of the service provider or regularly review the service provider's internal or external audit scope and findings. Service providers should have an effective internal audit function or should commission comprehensive, regular audits from a third-party organization. The reports of external auditors are commonly based on the AICPA's Statement of Auditing Standards [SAS] No. 70 "Reports on the Processing of Transactions by Service Organizations," as amended by SAS No. 78, "Consideration of Internal Control in a Financial Statement Audit: An Amendment to Statement on Auditing Standards No. 55." These statements contain the external-auditor reporting tools commonly used for service providers. SAS 70 reports,

20. When the service provider is affiliated with the serviced institution, sections 23A and 23B of the Federal Reserve Act may apply. In particular, section 23B provides that the terms of transactions between a bank and its nonbank affiliate must be comparable to the terms of similar transactions between nonaffiliated parties.

21. Additional information regarding common contract provisions can be found later in this section and in the FFIEC's *IT Handbook*. In addition, FFIEC Supervisory Policy SP-5 requires each serviced institution to evaluate the adequacy of its service provider's contingency plans.

however, should not be relied on to the same extent as an audit. There are two types of SAS 70 reports:

- *Reports on controls placed in operation* is an auditor's report on a service oganization's description of the controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements. It also reports on whether such controls were suitably designed to achieve specified control objectives. Lastly, it reports on whether the controls had been placed in operation as of a specific date.
- *Reports on controls placed in operation and tests of operating performance* is an auditor's report on a service organization's controls as described above, but the report also includes information on whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified.

Audit results, audit reports, and management responses must be available to examiners upon request.

8. *Contingency plans.* The serviced institution should ensure adequate business-resumption planning and testing by the service provider. When appropriate based on the scope and risks of the outsourced function and the condition and performance of the service provider, the serviced institution's contingency plan may also include plans for the continuance of processing activities, either in-house or with another provider, in the event that the service provider is no longer able to provide the contracted services or the arrangement is otherwise terminated unexpectedly.

International Considerations

In general, the arrangements for outsourcing critical information- or transaction-processing functions to service providers outside the United States should be conducted according to the risk-management guidelines described above. In addition, the Federal Reserve expects that these arrangements will not diminish the ability of U.S. supervisors to effectively review the domestic or foreign operations of U.S. banking organizations and the U.S. operations of foreign banking organizations. In particular, examiners should evaluate the adequacy of outsourcing arrangements in the following six areas:

1. *Oversight and compliance.* The institution is expected to demonstrate adequate oversight of a foreign service provider, such as through comprehensive audits conducted by the service provider's internal or external auditors, the institution's own auditors, or foreign bank supervisory authorities. The arrangement must not hinder the ability of the institution to comply with all applicable U.S. laws and regulations, including, for example, requirements for accessibility and retention of records under the Bank Secrecy Act. (See FinCEN's rule at 31 CFR 1020.320. See also section 208.62 of the Board's Regulation H (12 CFR 208.62) for suspicious-activity reporting and section 208.63 (12 CFR 208.63) for the Bank Secrecy Act compliance program.)
2. *Information access.* The outsourcing arrangement should not hinder the ability of U.S. supervisors to reconstruct the U.S. activities of the organization in a timely manner, if necessary. Outsourcing to jurisdictions where full and complete access to information may be impeded by legal or administrative restrictions on information flows will not be acceptable unless copies of records pertaining to U.S. operations are also maintained at the institution's U.S. office.
3. *Audit.* Copies of the most recent audits of the outsourcing arrangement must be maintained in English at the institution's U.S. office and must be made available to examiners upon request.
4. *Contingency plan.* The institution's contingency plan must include provisions to ensure timely access to critical information and service resumption in the event of unexpected national or geographic restrictions or disruptions affecting a foreign service provider's ability to provide services. Depending on the scope and risks of the outsourced function, this may necessitate backup arrangements with other U.S. or foreign service providers in other geographic areas.
5. *Foreign banking organizations.* With the exception of a U.S. branch or agency of a foreign bank that relies on the parent organization for information- or transaction-processing services, foreign banking organizations should maintain at the U.S. office

documentation of the home office's approval of outsourcing arrangements supporting its U.S. operations, whether to a U.S. or foreign service provider. The organization's U.S. office should also maintain documentation demonstrating appropriate oversight of the service provider's activities, such as written contracts, audit reports, and other monitoring tools. When appropriate, the Federal Reserve will coordinate with a foreign banking organization's home-country supervisor to ensure that it does not object to the outsourcing arrangement.

6. *Foreign branches or subsidiaries of U.S. banks and Edge corporations.* Documentation relating to outsourcing arrangements of the foreign operations of U.S. banking organizations with foreign service providers should be made available to examiners upon request.

INFORMATION-PROCESSING ENVIRONMENT

Many factors influence an institution's decision about whether to use internal or external data processing services, including the initial investment, operating costs, and operational flexibility. Historically, small financial institutions, which usually lack the funds or transaction volume to justify an in-house information system, were the chief users of external data processing companies. However, as advances in technology have decreased the cost of data processing, small institutions have become much more willing to invest in an in-house information system. At the same time, some financial institutions with internal information systems have discovered that they can save money by using external data processing companies for certain banking applications. Other financial institutions have engaged national companies or facilities-management organizations to assume their processing operations, while certain holding companies have organized their data processing departments as subsidiaries to centralize operations for their affiliate institutions.

The decision to establish an internal data processing center is a major one. Any bank's board of directors and management considering such a decision should thoroughly review and consider alternatives before proceeding. While a bank may gain a number of competitive advantages from an in-house facility, there are also many risks associated with this decision. Technological advances have reduced the price of small computer networks and made them more affordable, but banks should not use this as the sole justification for an internal data processing center.

A comprehensive feasibility study should precede any decision to develop an in-house system. This study should describe the costs, benefits, and risks and also give management the opportunity to compare current and future needs with existing abilities. The FFIEC's *IT Handbook* contains a complete discussion of feasibility studies.

The management of a financial institution must carefully identify the organization's needs for data processing. After these needs are properly identified (including the customers' needs for these services), management must carefully evaluate how the institution can best meet them. The costs and complexity of changing data processing arrangements can be substantial, so management must ensure that all related costs and benefits are identified and considered before deciding on a service. The following are the major external providers of data processing and IT services for financial institutions.

Correspondent Banks

Small financial institutions sometimes receive their IT services from a major correspondent bank. These services may be just one of a host of services available from the correspondent. Historically, the correspondent bank has been the least expensive servicer for many institutions. Correspondent banks may offset some of their own IT costs by using their excess processing capacity to provide services to correspondents.

Affiliated Financial Institutions and Banking Organizations

IT departments in holding companies or subsidiaries are one common form of an affiliated servicer. An affiliated data center may offer cost savings to other affiliates, since all parties are generally using the same software system. The serviced institutions can eliminate the duplication of tasks, and the affiliated data center and the overall organization can realize cost savings

through economies of scale. Thus, charges for IT services to affiliates are generally very competitive.

Regulatory guidelines strictly govern IT-servicing arrangements between affiliated institutions. Sections 23A and 23B of the Federal Reserve Act (12 U.S.C. 371c and 371c-1) address the question of allowable transactions between affiliates. This statute also states that the terms of transactions between affiliated parties must be comparable to the terms of similar transactions between nonaffiliated parties. An affiliated data center is allowed to set fees to recover its costs or to recover its costs plus a reasonable profit, or to set charges for data processing services that are comparable to those of a nonaffiliated servicer. Other restrictions may also apply.

Independent Service Bureaus

Independent service bureaus are present in most areas, but mergers and acquisitions have caused the number of bureaus to decline. When management investigates a service bureau's operations, it should determine if the servicer is familiar with the IT needs of financial institutions. Determining the percentage of the service bureau's business that comes from financial institutions will help the institution select a vendor that specializes in this type of processing. Independent service bureaus are normally responsive to user requests for specialized programs, since developing these programs for clients is generally a significant source of revenue. Tailoring a software program to a particular institution's needs becomes less attractive to the independent service bureau if the institution accounts for only a small portion of the bureau's workload or if the bureau offers a standardized software package as its primary product. However, some standardized software systems allow a modest amount of processing and report adjustments without requiring servicer modifications. Also, report-generator software, which provides clients with customized reports they can prepare without any help from the service bureau, is sometimes available from service bureaus.

Cooperative Service Corporations

A cooperative service corporation is a data processing facility formed by a group of financial institutions that agrees to share the operating costs. Under the right circumstances, this arrangement works well. For this strategy to succeed, however, all members of the group must be the same approximate size and have similar IT requirements. Typically, each institution owns a share of the facility or bears a share of the costs on a pro rata basis through investment in a bank service corporation. There must be a strong working relationship among the institutions. Although the institutions are not directly involved in the data processing center's daily operations, they are ultimately responsible for the center's success or failure.

One advantage of a cooperative service corporation is that individual institutions have increased control over the design of the data processing operation. Therefore, institutions can tailor computerized applications to meet their own needs. Resource pooling often provides for economies of scale as well, and cooperative ventures normally attract more highly skilled and more experienced employees.

Facilities-Management Providers

Medium- and large-sized financial institutions that already have an in-house data processing facility are the most likely users of facilities-management (FM) contracts. Small institutions typically do not have the work volume that is a prerequisite to hiring an FM company. Service contracts with FM companies are usually for a minimum term of five years, during which time the FM company assumes full responsibility for the institution's data processing operations. The institution pays the FM company a monthly fee to reimburse it for the costs of providing IT services plus a profit. The FM company usually carries out its tasks in the institution's former data processing center.

Financial institutions have various reasons for using FM companies, such as controlling or reducing the growth of data processing costs, ensuring better management of data center personnel, or using more modern software systems. Management of financially strained institutions may enter into FM arrangements to augment

their capital position by selling their equipment or facilities to the FM company.

Although an institution's contract with an FM company may provide a quick and easy solution to data processing problems with minimal involvement of senior officials, management should be aware of potential problems. FM contracts can have clauses that require the institution to pay more for services as work volume grows and can also contain provisions for periodic increases. The contract may include a substantial penalty for cancellation. Another risk is that the FM company may make personnel changes that are not advantageous to the institution, such as reassigning its best workers elsewhere or reducing the size of the data processing staff. Bank management should make sure that FM service contracts contain specific quality-measurement clauses and should monitor the quality of data processing services provided.

Other Purchased Services

Computer Time

A financial institution that designed its own data processing system and that maintains its own files only needs to rent computer time from an external servicer. This arrangement usually occurs when the financial institution's equipment or schedule makes it unable to handle some unusual processing task.

Time-Shared Computer Services

Most external providers of time-sharing services have a library of standardized programs available to any user. A user also may generate programs and store them in a reserved library. Financial institutions frequently use time-sharing services for financial analysis rather than recordkeeping. Applications with low input and output requirements and repetitive calculations, such as those required for a securities portfolio, lend themselves to a time-sharing arrangement. The external servicer in this arrangement normally does not maintain the client institution's data files. Financial institutions that store master files on the external servicer's equipment should maintain adequate documentation to facilitate the examination process. Under this arrangement, management should be concerned about ensuring logical and physical access to the terminal and about the availability of audit trails that indicate who has made changes to master files. Management should establish and monitor controls over passwords, terminals, and access to master files. For a complete discussion of controls over passwords and terminals, see the FFIEC's *IT Handbook.*

Satellite Processing

Satellite (remote) processing has become popular with some financial institutions that are located far away from an external servicer and that must process a large volume of transactions. A distinguishing characteristic of satellite processing is that the institution and the data center each perform a portion of the processing. Although the institution collects the data and sometimes prepares reports, the servicer makes the necessary master-file updates. To capture data and print reports, the serviced institution must acquire a terminal-entry device, a printer, an MICR reader/sorter, and a tape or disk unit. Since the system is usually online, the serviced institution must install modems and communications lines linking it to the servicer. The level of skill necessary to perform remote job entry in a satellite system is less sophisticated than the level needed to operate an in-house system. Most of the traditional control functions remain at the institution. The FFIEC's *IT Handbook* contains further information on satellite processing, remote job entry, and distributive processing systems.

Standard Program Packages

Most bank data centers and service bureaus specialize in processing one or more standard software packages. By using the same software for several users, external servicers achieve certain operating economies, which allow them to recover initial development costs more quickly. Most standard software packages are parameter driven, providing the user with some degree of flexibility. For example, in demand deposit and savings applications, standard program modules or common subroutines often allow the user to designate the format and frequency of reports. In addition, the user may select the parameters necessary to generate cer-

tain reports, such as the number of inactive days before an account becomes dormant or the minimum dollar amount for checks listed on the large-item report. The user can also be involved in selecting the criteria for interest rates, balance requirements, and other operating values, allowing for a tailored application within a standardized software system.

Tailored Applications

If standard program packages do not meet a financial institution's needs, an external servicer can be hired to design tailored applications to process the institution's data. The institution must clearly describe the proposed system and its operations to the servicer. Internal or external auditor participation in reviewing controls is also advisable. The initial cost of this approach is high, as are the costs of maintaining and updating the tailored applications.

OPERATIONAL AND TECHNOLOGICAL USER CONTROLS

Using computerized programs and networks, banks maintain a large number of accounts and record a high volume of transactions every day. Text-processing systems store vast amounts of correspondence. Transmission of data and funds regularly occurs over public communications links, such as telephone lines and satellite networks. The use of new technologies to transfer funds and records, while improving customer service and the institution's internal operations, has increased the potential for errors and abuse, which can result in loss of funds, lawsuits arising from damaged reputations, improper disclosure of information, and regulatory sanctions.

Controls must be implemented to minimize the vulnerability of all information and to keep funds secure. Bank management must assess the level of control necessary in view of the degree of exposure and the impact of unexpected losses on the institution. Certain practices can strengthen information and financial security. The most basic practices are the implementation of sound policies, practices, and procedures for physical security, separation of duties, internal quality control, hardware and software access controls, and audits. Bank management should institute information security controls that are designed to—

- ensure the integrity and accuracy of management information systems;
- prevent unauthorized alteration during data creation, transfer, and storage;
- maintain confidentiality;
- restrict physical access;
- authenticate user access;
- verify the accuracy of processing during input and output;
- maintain backup and recovery capability; and
- provide environmental protection against damage or destruction of information.

Although security features vary, they are usually available for all computer systems. The controls adopted should apply to information produced and stored by both automated and manual methods.

Written policies are generally recommended and, in most cases, institutions have chosen to establish and communicate security principles in writing. However, if an institution follows sound fundamental principles to control the risks discussed here, a written policy is not necessarily required. If sound principles are not effectively practiced, management may be required to establish written policies to formally communicate risk parameters and controls. Federal Reserve System policy does, however, require written contingency and disaster-recovery plans.

Examiners should regularly conduct reviews of information security. These reviews may include an assessment of—

- the adequacy of security practices,
- compliance with security standards, and
- management supervision of information security activities.

When conducting reviews of controls over information security, examiners must understand the difference between master files and transaction files. A master file is a main reference file of information used in a computer system, such as all mortgage loans. It provides information to be used by the program and can be updated and maintained to reflect the results of the processed operation. A transaction file or detail file contains specific transaction information, such as mortgage loan payments.

Manual Controls

The following discussion covers basic operational controls in a financial institution receiving external IT services. Similar controls should also be applied to information processed by an IT department within a user's own institution.

Separation of Duties

A basic form of operational control is separation of duties. With this control in place, no one person should be able to both authorize and execute a transaction, thereby minimizing the risk of undetected improper activities. Data center personnel should not initiate transactions or correct data except when it is necessary to complete processing in a reasonable time period. If this unusual situation arises, proper authorization should be obtained from data center and bank management. Both the servicer and the serviced institution should maintain documentation of these approvals, including details of the circumstances requiring the action. The same person normally should not perform input and output duties. However, in some instances, staff limitations may make one person responsible for several activities, such as—

- preparing batches and blocks or other input for entry to the system or shipment to the servicer;
- operating data entry equipment, including check reader/sorter machines, proof machines, or data-conversion devices;
- preparing rejects and nonreaders for reentry into the system;
- reconciling output to input or balancing the system;
- distributing output to ultimate users; and
- posting the general ledger and balancing computer output to the general ledger.

Rotation of assignments and periodic scheduled absences may improve internal controls by preventing one person from controlling any one job for an extended time period (and by providing cross-training and backup for all personnel). When vacations are scheduled, management may require staff to take uninterrupted vacations that are long enough to allow pending transactions to clear. These practices are most effective if vacations or other types of absences extend over the end of an accounting period or are for two consecutive weeks. Written policies and procedures may require job rotation.

Application manuals usually consist of a user's guide provided by the servicer that is supplemented by procedures written by the user. Manuals normally cover the preparation and control of source documents, certain control practices for moving documents or electronic images to and from the user and servicer, the daily reconcilement of totals to the general ledger, and master-file changes.

Management should implement dual control over automated systems. Personnel should place supervisory holds on customer accounts requiring special attention. For example, dormant accounts, collateral accounts, and accounts with large uncollected funds balances generally have holds that can be removed only by authorizations from two bank officials. In addition, certain types of transactions (for example, master-file changes) should require authorization from two bank officials by means of special codes or terminal keys. When employees add or remove a hold on an account or when the system completes a transaction requiring supervisory approval, the computer should generate an exception report. Assigned personnel not involved in the transaction should promptly review these reports for unusual or unauthorized activity.

Internal Quality Controls

Generally, there are three basic types of information systems, with many combinations and variations:

- *Inquiry-only system.* This system allows the user to search and review machine-readable records but not to alter them. Controls and security concerns related to this system are few; the major concern is unauthorized access to confidential information.
- *Memo-post system.* More sophisticated than the inquiry-only system, the memo-post system allows the user to create interim records. The servicer performs permanent posting routines using batch-processing systems. Controls for a memo-post system include limiting physical and logical access to the system and restricting certain transactions to supervisory personnel only. Appropriate levels of management should review memo-post reports daily.
- *Online-post system.* This system, sometimes

called a real-time system, requires the strictest controls. Online-post systems are vulnerable because all accepted transactions are transferred to machine-readable records. In addition to access controls, system reports should record all activity and exceptions. Appropriate levels of management should review these reports daily.

Internal controls fall into three general categories:

- *Administrative controls.* Administrative controls usually consist of management review of daily operations and output reports. Each application includes basic controls and exception reports that are common to all operations. To be effective, operations personnel must properly use exception reports and controls. This is especially true for controlling dormant accounts, check kiting, draws against uncollected funds, overdrafts, and the posting of computer-generated income and expense entries.
- *Dollar controls.* Dollar controls ensure processing for all authorized transactions. Operations personnel should establish work and control totals before forwarding data records to the data processor. Those same employees should not complete balancing procedures by reconciling trial balances to input, control sheets, and the general ledger. Report distribution should follow a formal procedure. Personnel should account for all rejects corrected and resubmitted.
- *Condoler controls.* Condoler controls are used when dollar values are not present in the data, as in name and address changes. Controls should be established before forwarding work for processing. Management should also implement procedures designed to ensure that its servicer processes all condoler transactions. For example, personnel should check new-account reports against new-account input forms or written customer-account applications to make sure that data are properly entered. To protect data integrity, management should develop procedures to control master-file and program changes. These procedures should also verify that the servicer is making only authorized changes and ensure that data processing employees do not initiate master-file changes.

Technological Controls

Encryption

Encryption is a process by which mathematical algorithms are used to convert plain text into encrypted strings of meaningless symbols and characters. This helps prevent unauthorized viewing and altering of electronic data during transmission or storage. The industry commonly uses the Data Encryption Standard (DES) for encoding personal identification numbers (PINs) on access cards, storing user passwords, and transferring funds on large-dollar payment networks.

Message-Authentication Code

A message-authentication code (MAC) is a code designed to protect against unauthorized alteration of electronic data during transmission or storage. This code is used with data encryption to further secure the transmission of large-dollar payments.

User Passwords

User passwords consist of a unique string of characters that a programmer, computer operator, or user must supply before gaining access to the system or data. These are individual access codes that should be specific to the user and known only to the user. Other security features of passwords should, at a minimum, require the users to change them periodically and store them in encrypted files. In addition, the passwords should be composed of a sufficient number of alphanumeric characters to make them difficult to guess. User passwords should not be displayed during the access process and should not be printed on reports.

Security Software

Security software is software designed to restrict access to computer-based data, files, programs, utilities, and system commands. Some systems can control access by user, transaction, and terminal. The software can generate reports that log actual and attempted security violations as well as access to the system.

Restricted Terminals

Limiting certain types of transactions to certain terminals or groups of terminals can help reduce exposure to loss. The offsetting problem is that loss of the ability to use these terminals can stop processing for an entire application. Bank management should therefore evaluate both the exposure and processing risks.

An automatic time-out feature can minimize the exposure risk. Since unauthorized users may target an unattended terminal, this feature automatically signs off the user when there has been no activity for a certain period of time. Using time-of-day restrictions can also limit unauthorized use of terminals during periods when an entire department or section would be unattended.

Restricted Transactions

Restricted transactions are specialized transactions that can be performed only by supervisory or management personnel. Examples include reversing transactions, dollar adjustments to customer accounts, and daily balancing transactions. Management should periodically review user needs and the appropriateness of restricting the performance of these transactions. System-generated reports can be used to review this activity more frequently.

Activity and Exception Reports

Report output will vary, depending on the sophistication of the data communications and applications software. Management should receive activity reports that detail transactions by terminal, operator, and type. More sophisticated software will produce activity and exception reports on other criteria, such as the number of inquiries by terminal, unsuccessful attempts to access the system, unauthorized use of restricted information, and any unusual activities (that is, infrequently used transactions).

Activity reports are used to monitor system use and may not be printed daily. However, management should periodically review and summarize these reports in an effort to ensure that machines are used efficiently. Exception reports should be produced and reviewed daily by designated personnel who have no conflicting responsibilities. A problem with many reporting systems is that the log contains a record of every event, making it cumbersome and more difficult to identify problems.

Controls over Software-Program-Change Requests

Requests for system changes, such as software-program changes, should be documented on a standard change-request form. The form is used to describe the request and document the review and approval process. It should contain the following information:

- date of the change request
- sequential control number
- program or system identification
- reason for the change
- description of the requested change
- person requesting the change
- benefits contemplated from the change
- projected cost
- signed approval authorizing the change including, at a minimum, the user, IT personnel with the proper authority, and an auditor (at least for significant changes)
- name of programmer assigned to make the change
- anticipated completion date
- user and information systems approval of the completed program change
- implementation procedures (steps for getting the program into the production library)
- audit review of change (if deemed necessary)
- documented sign-off

End-User Computing

End-user computing results from the transfer of information-processing capabilities from centralized data centers onto the user's desktop. End-user computing systems may range in size and computing power from laptop notebook computers to standalone personal computers, client server networks, or small systems with sufficient computing power to process all significant applications for a financial institution. Small systems that are entirely supported by a hardware or software vendor are referred to as turnkey systems. Control considerations discussed throughout this subsection generally apply to all end-user computing systems.

In many cases, end-user systems are linked by distributed processing networks. Linking several microcomputers together and passing information between them is called networking. A system configured in this manner is commonly called a local area network (LAN). The ability to decentralize the data processing function is largely a result of the development of powerful microcomputers or PCs. Microcomputers are now powerful enough to process significant applications when used as standalone systems. These microcomputers can also be connected to a host computer and configured to serve as a data entry or display terminal. In this terminal-emulation mode, information can be passed between the host and the PC with the processing occurring at either machine.

When linked by a network, end-user computing offers several advantages to financial institutions, including—

- low cost compared with other platforms,
- efficiency through the sharing of resources,
- ease of expansion for future growth,
- enhanced communication capabilities,
- portability,
- data availability, and
- ease of use.

While end-user computing systems provide several advantages, they also have greater risks to data integrity and data security, including—

- difficulty in controlling access to the system and in controlling access to confidential information that may be stored on individual personal computers and not on the system (such as payroll records, spreadsheets, budgets, and information intended for the board of directors of the financial institution),
- the lack of sophisticated software to ensure security and data integrity,
- insufficient capabilities to establish audit trails,
- inadequate program testing and documentation,
- lack of segregated duties of data entry personnel.

As the trend toward distributed processing continues, financial institutions should have proper policies, procedures, and reporting to ensure the accurate and timely processing of information. The controls governing access in an end-user computing environment should be no less stringent than those used in a traditional mainframe environment. Strict rules should govern the ability of users to access information. As a general rule, no user should be able to access information that is beyond what is needed to perform the tasks required by his or her job description. In this new environment, management and staff should assume responsibility for the information assets of the organization.

CONTINGENCY PLANNING, RECORD PROTECTION, AND RETENTION

Data communications systems are susceptible to software, hardware, and transmission problems that may make them unusable for extended periods of time. If a financial institution depends on data communication for its daily operations, appropriate back-up provisions are necessary. Back-up is the ability to continue processing applications in the event the communications system fails. Management can provide back-up by various methods, including batch-processing systems, intelligent terminals or PCs operating in an off-line mode, data capture at the controller if transmission lines are lost, redundant data communication lines, and back-up modems.

Regardless of the method used, FFIEC interagency issuances and specific supporting Federal Reserve System policy issuances that address corporate contingency planning require a comprehensive back-up plan with detailed procedures. When using a batch back-up system, operations personnel must convert data to a machine-readable format and transport the data to the servicer. This process may require additional personnel (data-entry operators and messengers) and equipment. An institution's contingency plan should include detailed procedures on how to obtain and use the personnel and equipment. Because on-line systems are updated or improved frequently, a batch back-up may not remain compatible. Institution personnel should perform periodic tests of batch and other back-up capabilities to ensure that protection is available and that employees are familiar with the plan.

Institutions should create computerized back-up copies of the institution's critical records and have alternative methods of processing those records. When IT operations are performed outside the institution, both the servicer and the financial institution should have adequate control over the records. Bank management

should determine which records are best protected by the servicer and which are best protected internally. Service contracts should outline the servicer's responsibility for storing bank records. If the servicer does not or will not permit specific reference to record retention in the contract, a general reference may be sufficient. The institution should obtain a copy of the servicer's back-up policy and retention procedures, and bank management should thoroughly understand which records are protected by whom and to what extent.

The bank should also review the servicer's software and hardware back-up arrangements. It should review the service provider's contingency plan and results of routine tests of the contingency plan. The review should determine how often data and software back-ups are made, the location of stored materials, and which materials are stored at that site. Management should also determine the availability of software replacement and vendor support, as well as the amount and location of duplicate software documentation. Software replacement and documentation procedures should be developed for both operating and application systems.

Management should review the servicer's hardware back-up arrangements to determine if (1) the servicer has a contract with a national recovery service and, if so, the amount and type of back-up capacity provided under the contract; (2) the servicer has an alternate data center with sufficient capacity and personnel to provide full service if necessary; or (3) multiple processing sites within the same facility are available for disaster-processing problems and if each site has an alternate power supply. The alternate site should be able to provide continued processing of data and transmission of reports.

Contracts or contingency plans should specify the availability of source documentation in the event of a disaster, including insolvency of the servicer. FFIEC interagency issuances and Federal Reserve System policy statements require financial institutions to evaluate the adequacy of a servicer's contingency plan and to ensure that its own contingency plan is compatible with the servicer's plan.

Since the duplication of records may vary from site to site, most organizations develop schedules for automatic retention of records on a case-by-case basis. The only way to ensure sufficient record protection is to continually review the flow of documents, data, and reports. Some records may be available in both hard-copy and machine-readable formats. In addition to determining the types of back-up records, management should determine whether it is possible to re-create current data from older records. Certain records also have uses apart from their value in reconstructing current data, such as meeting institutional and regulatory reporting requirements. These records usually include month-end, quarter-end, and year-end files.

The location of an external data center is another factor to consider when evaluating retention procedures. If the external data center is located in a building adjacent to the institution, the possibility that a disaster may affect both organizations increases. Such a situation may make off-site storage of back-up materials even more important. If, on the other hand, the serviced institution is located far from the data center, physical shipment of both input and output may become necessary. Management should determine if fast, reliable transportation between the two sites is available.

If a major disaster occurs, an alternate facility may not be available to process duplicated machine-readable media. Management should consider remote record storage that would facilitate the manual processing of records, if necessary. Furthermore, microfilming all items before shipment would protect the institution if any items are lost, misplaced, or destroyed. Optical-disk storage, which involves scanning and storing a document electronically, offers another alternative for storage and retrieval of original data after processing has occurred. The FFIEC's *IS Handbook* and related FFIEC and Federal Reserve System issuances are sources of information about planning for unexpected contingencies.

Processing personnel should regularly copy and store critical institution records in an off-site location that is sufficiently accessible to obtain records in a reasonable time period. These records should include data files, programs, operating systems, and related documentation. This also applies to critical data in hard-copy documents. In addition, an inventory of the stored information should be maintained along with a defined retention period.

AUDITS

Examiners need to determine the appropriateness of the scope and frequency of audit activi-

ties related to information systems and the reliability of internal or third-party audits of servicer-processed work. Furthermore, examiners should review the methods by which the board of directors is apprised of audit findings, recommendations, and corrective actions taken. In reviewing audit activities, examiners should consider the following factors (if applicable):

- the practicality of the financial institution's having an internal IT auditor and, if the institution has an internal IT auditor, the auditor's level of training and experience
- the training and experience of the institution's external auditors
- the audit functions performed by the institution's outside auditors, the servicer, the servicer's outside auditor, and supervisory personnel
- internal IT audit techniques currently being followed

The audit function should review controls and operating procedures that help protect the institution from losses caused by irregularities and willful manipulations of the data processing system. Thus, a regular, comprehensive audit of IT activities is necessary. Additionally, designated personnel at each serviced institution should periodically perform "around-the-computer" audit examinations, such as:

- developing data controls (proof totals, batch totals, document counts, number of accounts, and prenumbered documents) at the institution before submitting data to the servicer and sampling the controls periodically to ensure their accuracy;
- spot-checking reconcilement procedures to ensure that output totals agree with input totals, less any rejects;
- sampling rejected, unpostable, holdover, and suspense items to determine why they cannot be processed and how they were disposed of (to make sure they were properly corrected and re-entered on a timely basis);
- verifying selected master-file information (such as service-charge codes), reviewing exception reports, and cross-checking loan extensions to source documents;
- spot-checking computer calculations, such as the dollar amounts of loan rebates, interest on deposits, late charges, service charges, and past-due loans, to ensure proper calculations;
- tracing transactions to final disposition to ensure audit trails are adequate;
- reviewing source documents to ascertain whether sensitive master-file change requests were given the required supervisory approval;
- assessing the current status of controls by either visiting the servicer or reviewing independent third-party reviews of the servicer;
- reviewing processing procedures and controls; and
- evaluating other audits of the servicer.

In addition, "through-the-computer" audit techniques allow the auditor to use the computer to check data processing steps. Audit software programs are available to test extensions and footings and to prepare verification statements.

Regardless of whether an institution processes data internally or externally, the board of directors must provide an adequate audit program for all automated records. If the institution has no internal IT audit expertise, the nontechnical "around-the-computer" methods will provide minimum coverage, but not necessarily adequate coverage. A comprehensive external IT audit, similar to those discussed in the FFIEC's *IS Handbook*, should be carried out to supplement nontechnical methods.

INSURANCE

A financial institution should periodically review its insurance coverage to ensure that the amount of coverage is adequate to cover any exposure that may arise from using an external IT provider. To determine what coverage is needed, the institution should review its internal operations, the transmission or transportation of records or data, and the type of processing performed by the servicer. This review should identify risks to data, namely the accountability for data, at both the user and servicer locations and while in transit. Insurance covering physical disasters, such as fires, floods, and explosions, should be sufficient to cover replacement of the data processing system. Coverage that protects specialized computer and communications equipment may be more desirable than the coverage provided by regular hazard insurance. Expanded coverage protects against water infiltration, mechanical breakdown, electrical disturbances, changes in temperature, and corrosion. The use of an "agreed-amount" endorsement can provide for full recovery of covered loss.

Bank management should also review the servicer's insurance coverage to determine if the amounts and types are adequate. Servicer coverage should be similar to what the financial institution would normally purchase if it were performing its data processing internally. Servicer-provided coverage should complement and supplement the bank's coverage.

If a loss is claimed under the user's coverage, the user need only prove that a loss occurred to make a claim. However, if the loss is claimed under the servicer's coverage, the institution must prove that a loss occurred and also that the servicer was responsible for the loss.

Examiners should review the serviced institution's blanket bond coverage, as well as similar coverage provided by the servicer. The coverage period may be stated in terms of a fixed time period. The loss, the discovery, and the reporting of the loss to the insurer must occur during that stated period. Extended discovery periods are generally available at additional cost if an institution does not renew its bond. The dollar amount of the coverage now represents an aggregate for the stated period. Each claim paid, including the loss, court costs, and legal fees, reduces the outstanding amount of coverage, and recoveries do not reinstate previous levels of coverage. Since coverage extends only to locations stated in the policy, the policy must individually list all offices. Additionally, policies no longer cover certain types of documents in transit.

The bank's board of directors should be involved in determining insurance coverage since each board member will be acknowledging the terms, conditions, fees, riders, and exclusions of the policy. Insurance companies consider any provided information as a warranty of coverage. Any omission of substantive information could result in voided coverage.

The bank or servicer should consider buying additional coverage. Media-reconstruction policies defray costs associated with recovering data contained on the magnetic media. Media-replacement policies replace blank media. Extra-expense policies reimburse organizations for expenses incurred over and above the normal cost of operations. In addition, servicers often purchase policies covering unforeseen business interruptions and the liabilities associated with errors and omissions. Both servicer and banking organizations may purchase transit insurance that covers the physical shipment of source documents. Additionally, electronic funds transfer system (EFTS) liability coverage is available for those operations that use electronic transmission.

Several factors may influence an institution's decision to purchase insurance coverage or to self-insure: the cost of coverage versus the probability of occurrence of a loss, the cost of coverage versus the size of the loss of each occurrence, and the cost of coverage versus the cost of correcting a situation that could result in a loss. Some institutions engage risk consultants to evaluate these risks and the costs of insuring against them.

SERVICE CONTRACTS

Contract Practices

A poorly written or inadequately reviewed contract can be troublesome for both the serviced financial institution and the servicer. To avoid or minimize contract problems, bank legal counsel who are familiar with the terminology and specific requirements of a data processing contract should review it to protect the institution's interests. Since the contract likely sets the terms for a multiyear understanding between the parties, all items agreed on during negotiations must be included in the final signed contract. Verbal agreements are generally not enforceable, and contracts should include wording such as "no oral representations apply" to protect both parties from future misunderstandings. The contract should also establish baseline performance standards for data processing services and define each party's responsibilities and liabilities, where possible.

Although contracts between financial institutions and external data processing companies are not standardized in a form, they share a number of common elements. For a further discussion of IT contract elements and considerations, see the FFIEC's *IS Handbook*.

Additionally, section 225 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) states, "An [FDIC-] insured depository institution may not enter into a written or oral contract with any person to provide goods, products or services to or for the benefit of such depository institution if the performance of such contract would adversely affect the safety or soundness of the institution." An institution should ascertain during contract

negotiations whether the servicer can provide a level of service that meets the needs of the institution over the life of the contract. The institution is also responsible for making sure it accounts for each contract in accordance with GAAP. Regulatory agencies consider contracting for excessive servicing fees and/or failing to properly account for such transactions an unsafe and unsound practice. When entering into service agreements, banks must ensure that the method by which they account for such agreements reflects the substance of the transaction and not merely its form. See FFIEC Supervisory Policy SP-6, "Interagency Statement on EDP Service Contracts."

Risk of Termination

Many financial institutions have become so dependent on outside data processing servicers that any extended interruption or termination of service would severely disrupt normal operations. Termination of services generally occurs according to the terms of the service contract. Banks may also experience an interruption of services that is caused by a physical disaster to the servicer, such as a fire or flood, or by bankruptcy. The serviced institution must prepare differently for each type of termination. The contract should allow either party to terminate the agreement by notifying the other party 90 to 180 days in advance of the termination date, which should give a serviced institution adequate time to locate and contract with another servicer.

Termination caused by physical disaster occurs infrequently, but it may present the institution with a more serious problem than termination by contract. However, if the servicer has complied with basic industry standards and maintains a proper contingency plan, disruption of services to users will ordinarily be minimal. The contingency plan must require the servicer to maintain current data files and programs at an alternate site and arrange for back-up processing time with another data center. At a minimum, these provisions should allow the servicer to process the most important data applications. Since equipment vendors can often replace damaged machines within a few days, the servicer should be able to resume processing with little delay. The servicer, not the serviced institution, is responsible for the major provisions of its back-up contingency plan. However, the institution must have a plan that complements the servicer's.

Termination caused by bankruptcy of the servicer is potentially the most devastating to a serviced institution. There may not be advance notice of termination or an effective contingency plan (because servicer personnel may not be available). In this situation, the serviced institution is responsible for finding an alternate processing site.

Although user institutions can ordinarily obtain data files from a bankrupt servicer with little trouble, the programs (source code) and documentation required to process those files are normally owned by the servicer and are not available to the user institutions. These programs are often the servicer's only significant assets. Therefore, a creditor of a bankrupt servicer, in an attempt to recover outstanding debts, will seek to attach those assets and further limit their availability to user institutions. The bankruptcy court may provide remedies to the user institutions, but only after an extended length of time.

An escrow agreement is an alternative to giving vendors sole control of the source code. In this agreement, which should either be part of the service contract or a separate document, the financial institution would receive the right to access source programs under certain conditions, such as discontinued product support or the financial insolvency of the vendor. A third party would retain these programs and related documents in escrow. Periodically, the financial institution should determine that the source code maintained in escrow is up-to-date, for example, an independent party should verify the version number of the software. Without an escrow agreement, a serviced institution has two alternatives: (1) pay off the creditor and hire outside specialists to operate the center or (2) convert data files to another servicer. Either alternative is likely to be costly and cause severe operating delays.

Institutions should normally determine the financial viability of its servicer annually. Once the review is complete, management must report the results to the board of directors or a designated committee. At a minimum, management's review should contain a careful analysis of the servicer's annual financial statement. Management may also use other sources of information to determine a servicer's condition, such as investment analyst reports and bond ratings.

Reports of independent auditors and examination reports for certain service providers obtainable from appropriate regulatory agencies may contain useful information.

AUTOMATED CLEARINGHOUSE

Automated clearinghouses (ACHs) form a nationwide electronic payments system used by a large number of depository institutions and corporations. ACH rules and regulations are established by the National Automated Clearing House Association (NACHA) and the local ACH associations, and they are referenced in the ACH operating circulars of the Federal Reserve Banks.

ACH is a value-based system that supports both credit and debit transactions. In ACH credit transactions, funds flow from the depository institution originating the transaction to the institutions receiving the transactions. Examples of credit payments include direct deposits of payroll, dividend and interest payments, Social Security payments, and corporate payments to contractors and vendors. In a debit transaction, funds flow from the depository institutions receiving the transaction instructions to the institution originating the transaction. Examples of ACH debit transactions include collection of insurance premiums, mortgage and loan payments, consumer bill payments, and transactions to facilitate corporate cash management. ACH transactions are deposited in batches at Federal Reserve Banks (or private-sector ACH processors) for processing one or two business days before the settlement date. These transactions are processed and delivered to the receiving institutions through the nightly processing cycle for a given day.

ACH transactions continue to grow significantly. Additional uses of the ACH continue to be developed as depository institutions, corporations, and consumers realize its efficiency and low cost compared with large-dollar payments systems and check payments. One area of growth is the use of debit transactions for the collection of large payments due to the originator, such as the cash concentration of a company's nationwide branch or subsidiary accounts into one central account and other recurring contractual payments.

While several organizations can be involved in processing ACH transactions, the Federal Reserve System is the principal ACH processor. For the Federal Reserve ACH system, depository institutions send ACH transactions to and receive ACH transactions from one of the Federal Reserve processing sites via a communications system linking each location. Access may be by direct computer interface or intelligent terminal connections.

As with any funds-transfer system, the ACH system has inherent risks, including error, credit risk, and fraud. When reviewing ACH activities, examiners should evaluate the following:

- agreements covering delivery and settlement arrangements maintained by the depository institution as an originator or receiver of ACH transactions
- monitoring of the institution's and customer's intraday positions
- balancing procedures of ACH transactions processed
- the credit policy and effectiveness of procedures to control intraday and overnight overdrafts, resulting from extensions of credit to an ACH customer, to cover the value of credit transfers originated (Since ACH transactions may be originated one or two days before the settlement date, the originating institution is exposed to risk from the time it submits ACH credit transfers to the ACH processor to the time its customer funds those transfers.)
- uncollected-funds controls and the related credit policy for deposits created through ACH debit transactions (ACH debits can be returned for insufficient funds in the payor's account or for other reasons, such as a court order.)
- exception reports (that is, large-item and new-account reports)
- control procedures for terminals through which additions, deletions, and other forms of maintenance could be made to customer databases
- the retention of all entries, return entries, and adjustment entries transmitted to and received from the ACH for a period of six years after the date of transmittal

RETAIL FUNDS-TRANSFER SYSTEMS

Automation has enabled banks to electronically perform many retail banking functions formerly handled manually by tellers, bookkeepers, data-

entry clerks, and other banking personnel. Accordingly, the need for physical banking facilities and related staff has been reduced. Electronic funds transfer (EFT) and related banking services have also brought access to and control of accounts closer to the consumer through the use of widely distributed unmanned terminals and merchant facilities. EFT-related risk to a financial institution for individual customer transactions is generally low, since the transactions are usually for relatively small amounts. However, weaknesses in controls that could lead to incorrect or improper use of several accounts could lead to significant losses or class action suits against a financial institution. Examinations of retail EFT facilities should focus on the potential large-scale risks of a given product. Examples of retail EFT systems include automated teller machines, point-of-sale networks, debit and "smart" cards, and home banking.

Automated Teller Machines

An automated teller machine (ATM) is a terminal that is capable of performing many routine banking services for the customer. ATMs handle deposits, transfers between savings and checking accounts, balance inquiries, withdrawals, small short-term loans, and loan payments. ATMs may also handle other transactions, such as cash advances on credit cards, statement printing, and postage-stamp dispensing. ATMs usually operate 24 hours a day and are located not only on bank premises but in other locations, such as shopping malls and businesses. Daily withdrawals are usually, and should be, limited to relatively small amounts ($200 to $500). Deposits are processed in the same manner as if they were handled by a teller. ATMs are generally activated through the use of a plastic card encoded with a machine-readable customer identification number and the customer's entry of a corresponding personal identification number (PIN). Some financial institutions may refer to this identification number as the personal identification code (PIC).

ATMs operate in either off-line or on-line mode. Off-line transactions are those that occur when the customer's account balance is not available for verification. This situation can be the result of telecommunication problems between the financial institution and the ATM network. In addition, an off-line transaction can occur when a customer's account balance is not available because the financial institution is updating its files. Financial institutions usually update their files during low-volume periods. In either case, transactions are usually approved up to the daily withdrawal limit, which is a risk to the bank because a customer can withdraw more than is available in the account. On-line systems are directly connected to a financial institution's computer system and the corresponding customer account information. The computer processes each transaction immediately and provides immediate account-balance verification. With either system, a card is normally captured (kept by the ATM) if misuse is indicated (for example, the card has been reported stolen or too many attempts have been made with an invalid PIN).

Financial institutions are usually members of several ATM networks, which can be regional and national. Through these networks, separate institutions allow each other's customers to use their ATM machines. This is known as an interchange system. To be involved in an interchange system, a financial institution must either be an owner or member of the ATM network.

Fraud, robbery, and malfunction are the major risks of ATMs. The use of plastic cards and PINs are a deterrent, but there is still the risk that an unauthorized individual may obtain them. Customers may even be physically accosted while making withdrawals or deposits at ATM locations. Institutions have decreased this risk by installing surveillance cameras and access-control devices. For example, the ATM card can be used as an access-control device, unlocking the door to a separate ATM enclosure and relocking it after the customer has entered. Fraud may also result from risks associated with the issuance of ATM cards, the capture of cards, and the handling of customer PINs. Appropriate controls are needed to prevent the financial institution's personnel from unauthorized access to unissued cards, PINs, and captured cards.

Point-of-Sale Systems

A point-of-sale (POS) system transaction is defined as an electronic transfer of funds from a customer's checking or savings account to a merchant's account to pay for goods or services. Transactions are initiated from POS terminals

located in department stores, supermarkets, gasoline stations, and other retail outlets. In an electronic POS system, a customer pays for purchases using a plastic card (such as an ATM, credit, or debit card). The store clerk enters the payment information into the POS terminal, and the customer verifies the transaction by entering a PIN. This results in a debit to the customer's account and a credit to the merchant's account.

POS transactions may be processed through either single-institution unshared systems or multi-institution shared networks. Participants in a shared system settle daily, on a net transaction basis, between each other. In unshared systems, the merchants and customers have accounts with the same financial institution. Thus, the need to settle between banks is eliminated.

As with other EFT systems, POS transactions are subject to the risk of loss from fraud, mistakes, and system malfunction. POS fraud is caused by stolen cards and PINs, counterfeit cards, and unauthorized direct computer access. The system is also susceptible to errors such as debiting or crediting an account by too much or too little, or entering unauthorized transactions. For the most part, POS systems usually deal with these risks by executing bank-merchant and bank-customer contracts that delineate each party's liabilities and responsibilities. Also, consumers are protected by state and federal statutes limiting their liability if they give notice of a lost, stolen, or mutilated card within a specified time period. Other risks inherent in POS systems are computer malfunction or downtime. Financial institutions offering POS services should provide for back-up of their records through adequate contingency planning. Internal control guidelines for POS systems should address the following:

- confidentiality and security of customer-account information, including protection of PINs
- maintenance of contracts between banks and merchants, customers and banks, and banks and networks
- policies and procedures for credit and check authorization, floor limits, overrides, and settlement and balancing
- maintenance of transaction journals to provide an adequate audit trail
- generation and review of daily exception reports with provisions for follow-up of exception items
- provisions for back-up and contingency planning
- physical security surrounding POS terminals

Internal Controls for Retail EFT Systems

Regardless of the EFT system employed, financial institutions should ensure that adequate internal controls are in place to minimize errors, discourage fraud, and provide an adequate audit trail. Recommended internal-control guidelines for all systems include:

- establishing measures to establish proper customer identification (such as PINs) and maintain their confidentiality
- installing a dependable file-maintenance and retention system to trace transactions
- producing, reviewing, and maintaining exception reports to provide an audit trail

The most critical element of EFT systems is the need for undisputed identification of the customer. Particular attention should be given to the customer-identification systems. The most common control is the issuance of a unique PIN that is used in conjunction with a plastic card or, for noncard systems, an account number. The following PIN control guidelines, as recommended by the American Bankers Association, are encouraged.

Storage:

- PINs should not be stored on other source instruments (for example, plastic cards).
- Unissued PINs should never be stored before they are issued. They should be calculated when issued, and any temporary computer storage areas used in the calculation should be cleared immediately after use.
- PINs should be encrypted on all files and databases.

Delivery:

- PINs should not appear in printed form where they can be associated with customers' account numbers.
- Bank personnel should not have the capability to retrieve or display customers' PIN numbers.

- All the maintenance to PINs stored in databases should be restricted. Console logs and security reports should be reviewed to determine any attempts to subvert the PIN security system.
- PIN mailers should be processed and delivered with the same security accorded the delivery of bank cards to cardholders. (They should never be mailed to a customer together with the card).

Usage:

- The PIN should be entered only by the cardholder and only in an environment that deters casual observation of entries.
- The PIN should never be transmitted in unencrypted form.
- PIN systems should record the number of unsuccessful PIN entries and should restrict access to a customer's account after a limited number of attempts.
- If a PIN is forgotten, the customer should select a new one rather than have bank personnel retrieve the old one, unless the bank has the ability to generate and mail a hard copy of the PIN directly to the customer without giving bank personnel the ability to view the PIN.

Control and security:

- Systems should be designed, tested, and controlled to preclude retrieval of stored PINs in any form.
- Application programs and other software containing formulas, algorithms, and data used to calculate PINs must be subject to the highest level of access control for security purposes.
- Any data-recording medium, for example, magnetic tape and removable disks, used in the process of assigning, distributing, calculating, or encrypting PINs must be cleared immediately after use.
- Employees with access to PIN information must be subject to security clearance and must be covered by an adequate surety bond.

System design:

- PIN systems should be designed so that PINs can be changed without reissuing cards.
- PINs used on interchange systems should be designed so that they can be used or changed without any modification to other participants' systems.
- Financial institutions electing to use encryption as a security technique for bank card systems are strongly encouraged to consider the data encryption standards established by the National Institute of Standards and Technology.

In addition, institutions should consider controls over other aspects of the process. Control guidelines appropriate for plastic cards include those covering procurement, embossing or encoding, storage, and mailing. Controls over terminal sharing and network switching are also appropriate. Institutions should address backup procedures and practices for retail funds-transfer systems and insurance coverage for these activities.

APPENDIX—INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

Sections II and III of the information security standards are provided below. For more information, see the Interagency Guidelines Establishing Information Security Standards, in Regulation H, section 208, appendix D-2 (12 CFR 208, appendix D-2). The guidelines were previously titled Interagency Guidelines Establishing Standards for Safeguarding Customer Information. The information security standards were amended, effective July 1, 2005, to implement section 216 of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act). To address the risks associated with identity theft, the amendments generally require financial institutions to develop, implement, and maintain, as part of their existing information security program, appropriate measures to properly dispose of consumer information derived from consumer reports. The term *consumer information* is defined in the revised rule.

II. Standards for Safeguarding Customer Information

A. Information Security Program

Each bank is to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities. While all parts of the bank are not required to implement a uniform set of policies, all elements of the information security program are to be coordinated. A bank is also to ensure that each of its subsidiaries is subject to a comprehensive information security program. The bank may fulfill this requirement either by including a subsidiary within the scope of the bank's comprehensive information security program or by causing the subsidiary to implement a separate comprehensive information security program in accordance with the standards and procedures in sections II and III that apply to banks.

B. Objectives

A bank's information security program shall be designed to—

1. ensure the security and confidentiality of customer information;
2. protect against any anticipated threats or hazards to the security or integrity of such information;
3. protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. ensure the proper disposal of customer information and consumer information.

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors

The board of directors or an appropriate committee of the board of each bank is to—

1. approve the bank's written information security program; and
2. oversee the development, implementation, and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk

Each bank is to—

1. identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems;
2. assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;
3. assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks; and
4. ensure the proper disposal of customer information and consumer information.

C. Manage and Control Risk

Each bank is to—

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:
   a. access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means
   b. access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals
   c. encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access
   d. procedures designed to ensure that customer information system modifications

are consistent with the bank's information security program
   e. dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information
   f. monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems
   g. response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies
   h. measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures
2. Train staff to implement the bank's information security program.
3. Regularly test the key controls, systems, and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.
4. Develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of customer information and consumer information in accordance with each of the requirements in this section III.

D. Oversee Service-Provider Arrangements

Each bank is to—

1. exercise appropriate due diligence in selecting its service providers;
2. require its service providers by contract to implement appropriate measures designed to meet the objectives of the information security standards; and
3. where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations with regard to the requirements for overseeing provider arrangements. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. Adjust the Program

Each bank is to monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board

Each bank is to report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with the information security standards. The reports should discuss material matters related to its program, addressing issues such as risk assessment; risk management and control decisions; service-provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. Implement the Standards

(For the effective dates, see 12 CFR 208, appendix D-2, section III.G.)

1. To explicitly consider IT when developing risk assessments and supervisory plans.
2. To assess the types and levels of risks associated with information technology.
3. To exercise appropriate judgment in determining the level of review, given the characteristics, size, and business activities of the organization.
4. To develop a broad understanding of the organization's approach, strategy, and structure for IT activities within and across business lines.
5. To assess the adequacy of IT architecture and the ability of the current infrastructure to meet operating objectives, including the effective integration of systems and sources of data.
6. To assess the adequacy of the system of controls to safeguard the integrity of the data processed in critical information systems.
7. To determine if the board has developed, implemented, and tested contingency plans that will ensure the continued operation of the institution's critical information systems.
8. To ensure that operating procedures and controls are commensurate with the potential for and risks associated with security breaches, which may be either physical or electronic, inadvertent or intentional, or internal or external.
9. To determine the scope and adequacy of the IT audit function.
10. To evaluate IT outsourcing risk and outsourcing arrangements involving major lines of business.
11. To determine if the institution is complying with its written information security program and the minimum governing interagency standards on information security; the guidelines on the proper disposal of consumer information; and all applicable laws, rules, and regulations.
12. To find out if the financial institution (the bank and its respective operating subsidiaries) has developed, implemented, and maintained a written Identity Theft Prevention Program (Program) for its new and existing accounts that are covered by the Fair and Accurate Transactions Act of 2003 (FACT Act) and the Federal Reserve Board's rules on Fair Credit Reporting, section 222, Subpart J—Identity Theft Red Flags (12 CFR 222, Subpart J), which implements provisions of the FACT Act.
13. To make a determination of whether the financial institution's Program is
    a. designed to detect, prevent, and mitigate identity theft in connection with the opening of a new, or an existing, covered account and that the Program includes the detection of relevant Red Flags;[1] and
    b. appropriate to the size and complexity of the financial institution and the nature and scope of its activities.
14. To ascertain whether the financial institution assesses the validity of change of address notifications that it receives for the credit and debit cards that it has issued to customers.
15. To prepare comments for the report of examination on significant deficiencies and recommended corrective action.
16. To assign a Uniform Rating System for Information Technology (URSIT) rating or determine the impact of IT risks on the CAMELS or risk ratings.
17. To update the workpapers with any information that will facilitate future examinations.

1. Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

1. Determine the role and importance of IT to the organization and whether any unique IT characteristics or issues exist. Identify and list or update the major automated banking applications. For those applications processed by outside service providers, indicate the name and location of each service provider.
2. Incorporate an analysis of IT activities into risk assessments, supervisory plans, and scope memoranda, considering the size, activities, and complexity of the organization, as well as the degree of reliance on these systems across particular business lines.
3. Assess the organization's critical IT systems—those that support its major business activities—and the degree of reliance those activities have on IT systems. (See the *FFIEC Information Systems Examination Handbook* for more information on reviewing the IT function.)
4. Determine if the systems are delivering the services necessary for the organization to conduct its business in a safe and sound manner.
5. Determine whether the board of directors and senior management are adequately identifying, measuring, monitoring, and controlling risks associated with IT for the overall organization and its major business activities.
6. Determine if the IT strategy for the significant business activities or the organization is consistent with the organization's mission and business objectives. Determine whether the IT function has effective management processes to execute that strategy.
7. Review the reliability, accuracy, and completeness of information delivered in key business lines.
8. Review the bank's information security program. Assess the adequacy of the organization's policies, procedures, and controls, as well as its compliance with them.
9. Determine the capability of backup systems, as presented in contingency plans, to mitigate business disruption.
10. Ascertain the quality and adequacy of the internal or external IT audit function or any independent application reviews to ensure the integrity, security, and availability of the organization's systems.
11. Complete or update the information technology internal control questionnaire (section 4060.4) for the specific applications identified in step 1 of these procedures, noting any of the following:
    a. internal control exceptions and noncompliance with written policies, practices, and procedures
    b. violations of law
    c. exceptions to IT-servicing contracts
    d. overall evaluation of services provided to the bank, including any problems experienced with the servicer
12. Complete or update the "Establishing Information Security Standards" portion of the internal control questionnaire. (See section 4060.4.) Examiners should use this information to assess an institution's compliance with the interagency information security standards and the guidelines for the proper disposal of consumer information. Depending on the nature of the institution's operations and the extent of prior supervisory review, all questions may not need to be answered fully. Other examination resources may also be used (for example, the *FFIEC Information Systems Examination Handbook*). Examiners should conduct a review that is a sufficient basis for evaluating the overall written information security program of the institution and its compliance with the interagency guidelines.
13. Verify that the financial institution has determined initially, and periodically thereafter, whether it offers or maintains accounts covered by the Fair and Accurate Transactions Act of 2003 (FACT Act) and section 222, Subpart J—Identity Theft Red Flags of the Board's rules on Fair Credit Reporting (12 CFR 222, Subpart J).
14. Determine if the financial institution has adequately developed and maintains a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and monitor transactions to mitigate identity theft in connection with the opening of certain new and existing accounts covered by the FACT Act.

15. Evaluate whether the Program includes reasonable policies and procedures to
    a. identify and detect relevant Red Flags[1] for the financial institution's covered accounts and whether it incorporated those Red Flags into its Program;
    b. respond appropriately to any detected Red Flags to prevent and mitigate identity theft; and
    c. ensure that the program is updated periodically to reflect changes in identity theft risks to customers and the safety and soundness of the financial institution.
16. If a required Program has been established by the financial institution, ascertain if it has provided for the Program's continued administration, including
    a. involving the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the continued oversight, development, implementation, and administration of the Program;
    b. training staff, as necessary, to effectively implement the Program; and
    c. appropriate and effective oversight of service provider arrangements; and
17. If the financial institution has established and maintains a required Program that applies to its covered accounts, determine if the institution's Program includes the relevant and appropriate guidelines within the rule's appendix J (12 CFR 222, appendix J).
18. Determine whether the institution's controls over outsourcing information- and transaction-processing activities are adequate. Evaluate the adequacy of controls over outsourcing arrangements in the following areas:
    a. outsourcing risk assessment
    b. selection of service providers
    c. contracts
    d. policies, procedures, and controls
    e. ongoing monitoring
    f. information access
    g. audit
    h. contingency plan
19. Determine whether the bank has properly notified the Federal Reserve Bank of new outsourced services in accordance with the Bank Service Corporation Act (12 U.S.C. 1865).
20. Review any recent IT reports of examination on the institution's service providers performed by the Federal Reserve or other regulatory authorities, and note any deficiencies. Obtain a listing of any deficiencies noted in the latest audit review. Determine that all deficiencies have been properly corrected.
21. For banks with material in-house processing, use the Uniform Rating System for Information Technology (URSIT) rating system to help evaluate the entity's overall risk exposure and risk-management performance. Evaluate the areas identified within each relevant URSIT component to assess the institution's ability to identify, measure, monitor, and control IT risks.
22. Determine the extent of supervisory attention needed to ensure that IT weaknesses are addressed and that associated risk is properly managed. Determine the impact on CAMELS, the operational-risk rating, and any other risk ratings.
23. Prepare comments for the report of examination on any significant deficiencies and recommended corrective action.
24. Update the workpapers with any information that will facilitate future examinations.

1. Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Information Technology
Internal Control Questionnaire
Effective date October 2008

Section 4060.4

Review the bank's internal controls, policies, practices, and procedures for information technology. The bank's system should be documented completely and concisely and should include, where appropriate, narrative description, flow charts, copies of forms used, and other pertinent information. Items below that are marked with an asterisk require substantiation by observation or testing.

SERVICER SELECTION

1. Before entering into any service arrangement, did management consider—
   a. alternative servicers and related costs?
   b. the financial stability of the servicer?
   c. the control environment at the data center?
   d. emergency backup provisions?
   e. the ability of the servicer to handle future processing requirements?
   f. requirements for termination of service?
   g. the quality of reports?
   h. insurance requirements?
2. Is there an annual reevaluation of the servicer's performance that includes—
   a. its financial condition?
   b. costs?
   c. its ability to meet future needs?
   d. its quality of service?

CONTRACTS

*1. Is each automated application covered by a written contract?
*2. Were contracts reviewed by legal counsel?
3. Does each service contract cover the following areas:
   a. ownership and confidentiality of files and programs?
   b. liability limits for errors and omissions?
   c. frequency, content, and format of input and output?
   d. the fee structure, including—
      • current fees?
      • provisions for changing fees?
      • fees for special requests?
   e. provisions for backup and record protection?
   f. the notice required (by either party) for termination of service and the return of customer records in a machine-readable form?
   g. time schedules for receipt and delivery of work, including processing priorities?
   h. the insurance carried by the servicer?
   i. liability for documents in transit?
   j. audit responsibility?
   k. a provision to supply the serviced institution with yearly financial statements (preferably audited with both consolidated and unconsolidated figures when applicable)?

INSURANCE

*1. Does the serviced institution's insurance coverage include the following provisions:
   a. extended blanket bond fidelity coverage to employees of the servicer?
   b. insurance on documents in transit, including the cash letter?
   c. if the serviced institution is relying on the servicer or an independent courier for the insurance described above, is adequate evidence of that coverage on file?

OPERATIONAL CONTROLS

*1. Are duties adequately separated for the following functions:
   a. input preparation?
   b. operation of data-entry equipment?
   c. preparation of rejects and unposted items for reentry?
   d. reconcilement of output to input?
   e. output distribution?
   f. reconcilement of output to general ledger?
   g. posting general ledger?
2. Are employee duties periodically rotated for control and training purposes?
3. Do supervisors or officers—
   a. adequately review exception reports?
   b. approve adjusting entries?

4. Are servicer personnel prohibited from initiating transactions or correcting data?
5. Are individuals prohibited from initiating or authorizing a transaction and then executing it?
6. Are employees at the serviced institution required to be absent from their duties (by vacation or job rotation) for two consecutive weeks?
7. Are master-file changes—
   a. requested in writing?
   b. approved by a supervisor?
   c. verified as correct after processing?

*8. Are exception reports prepared for—
   a. unposted and rejected items?
   b. supervisory-override transactions?
   c. master-file changes (before and after)?
   d. dormant-account activity?

*9. Does each user department—
   a. establish dollar and nondollar control totals before they are sent for processing?
   b. receive all scheduled output reports even when the reports contain no activity?
   c. review all output and exception reports?

*10. Are current user manuals available for each application, and do employees use them?

11. Does each user manual cover—
   a. preparation and control of source documents?
   b. control, format, and use of output?
   c. settlement and reconcilement procedures?
   d. error-correction procedures?

12. Are users satisfied with the servicer's performance and output reports? (If not, explain.)
13. Are computer-generated entries subsequently reviewed and approved by appropriate officials?

*14. Does the serviced institution copy all source documents, including cash letters, on microfilm before they leave the premises? If so—
   a. is the microfilm stored in a secure location with limited access?
   b. is an inventory and usage log maintained?

COMMUNICATION CONTROLS

*1. Is user access to the data communication network controlled by—
   a. user number?
   b. physical keys?
   c. passwords?
   d. other safeguards (explain)?

2. Are periodic changes made to numbers, keys, or passwords, and are they adequately controlled?
3. Are identification numbers or passwords suppressed on all printed output and video displays?
4. Are terminals controlled as to—
   a. what files can be accessed?
   b. what transactions can be initiated?
   c. specific hours of operations?

5. Do controls over restricted transactions and overrides include—
   a. supervisory approval?
   b. periodic management review?

*6. Are there exception reports that indicate—
   a. all transactions made at a terminal?
   b. all transactions made by an operator?
   c. restricted transactions?
   d. correcting and reversing entries?
   e. dates and times of transactions?
   f. unsuccessful attempts to gain access to the system or to restricted information?
   g. unusual activity?

7. Overall, are there adequate procedures in effect that prevent unauthorized use of the data communication systems?
8. To back up online systems—
   a. are offline capabilities available (explain)?
   b. are the offline capabilities periodically tested?

AUDITING

1. Is there an internal auditor or member of management not directly involved in EDP activities who has been assigned responsibility for the audit function?
2. Does that individual have any specialized audit or EDP training?
3. Are there written internal audit standards and procedures that require—
   a. review of all automated applications?
   b. reports to the board of directors?
   c. audit workpapers?
4. Does the person responsible for the

audit function perform the following procedures:
   a. test the balancing procedures of all automated applications, including the disposition of rejected and unposted items?
   b. periodically sample master-file information to verify it against source documents?
   c. spot-check computer calculations, such as interest on deposits, loans, securities, loan rebates, service charges, and past-due loans?
   d. verify output report totals?
   e. check accuracy of exception reports?
   f. review master-file changes for accuracy and authorization?
   g. trace transactions to final disposition to determine the adequacy of audit trails?
   h. review controls over program-change requests?
   i. perform customer confirmations?
   j. other (explain)?
5. Does the serviced institution obtain and review the servicer's internal or external audits or third-party reviews? (If yes, detail exceptions and corrective action.)
6. Has the serviced institution used an independent auditor to evaluate EDP servicing (if yes, detail exceptions and corrective action)?
7. Is the overall audit program for serviced applications considered adequate?

ESTABLISHMENT OF INFORMATION SECURITY STANDARDS

1. Does the bank have a written information security program or policy that complies with the Interagency Guidelines Establishing Information Security Standards, in Regulation H, appendix D-2 (12 CFR 208, appendix D-2)? Has the board of directors or an appropriate designated committee of the board approved the written information security program?
2. Is the written information security program appropriate given the size and complexity of the organization and its operations? Does the program contain the objectives of the program, assign responsibility for implementation, and provide methods for compliance and enforcement?
3. Does the bank periodically update its information security program to reflect changes in the bank's operations and systems, as well as changes in threats or risks to the bank's customer information?
4. Does the examination review of the bank's process for assessing risk to its customer information address the following questions:
   a. Has the bank identified the locations, systems, and methods for storing, processing, transmitting, and disposing of its customer information?
   b. Has the bank identified reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems, and has the bank assessed the likelihood of these threats and their potential damage to the bank and its customers?
5. With respect to the bank's risk-management processes for implementing effective measures to protect customer information, does the bank adopt and review appropriate risk-based internal controls and procedures for the following:
   a. accessing controls on computer systems containing customer information in order to prevent access by unauthorized staff or other individuals?
   b. preventing employees from providing customer information to unauthorized individuals, including "pretext calling," that is, someone calling a bank and posing as a customer to fraudulently obtain an individual's personal information? (See SR-01-11.)
   c. providing access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records-storage facilities, in order to permit access to authorized individuals only?
   d. encrypting electronic customer information, including information that is in transit or in storage on networks or systems, when unauthorized individuals are able to gain access to it?
   e. ensuring that modifications to customer information systems are consistent with the bank's information security program?

f. maintaining dual-control procedures, segregation of duties, and background checks for employees with access to customer information to minimize the risk of internal misuse of customer information?
g. monitoring systems and procedures to detect unauthorized access to customer information systems that could compromise the security of customer information?
h. maintaining and complying with the minimum requirements for response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems? (These programs include appropriate reports, such as Suspicious Activity Reports, disseminated to regulatory and law enforcement agencies.) See the requirements for suspicious-activity reporting in section 208.62 of the Board's Regulation H (12 CFR 208.62), and the Bank Secrecy Act compliance program in section 208.63 (12 CFR 208.63).
i. providing measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures?
j. providing measures to ensure the proper disposal of consumer information derived from consumer reports?

6. Have the bank's employees been trained to implement the information security program?
7. Does the bank regularly test the effectiveness of the key controls, systems, and procedures of its information security program? These tests may include, for example, tests of operational contingency plans, system security audits or "penetration" tests, and tests of critical internal controls over customer information. Are tests conducted and reviewed independently by the bank's designated staff?
8. Does the bank provide customer information to any service providers, or do any service providers have access to customer information as a result of providing services directly to the bank? If so—
   a. has the bank conducted appropriate due diligence in selecting its service providers, taking into consideration information security?
   b. do the bank's contracts with its service providers require implementation of appropriate information security programs and measures?
   c. where appropriate and based on risk, does the bank monitor its service providers to confirm that they are maintaining appropriate security measures to safeguard the bank's customer information? Does the bank, for example, conduct or review the results of audits, security reviews or tests, or other evaluations?
9. Does the bank's management report at least annually to the board of directors, or to a designated appropriate board committee, on the overall status of the information security program and the extent of the bank's compliance with the standards and guidelines?

IDENTITY THEFT RED FLAGS

1. Did the bank (financial institution) determine initially, and has it periodically determined, whether it offers or maintains accounts covered by the Fair and Accurate Transactions Act of 2003 (FACT Act) and section 222, Subpart J—Identity Theft Red Flags of the Board's rules on Fair Credit Reporting (12 CFR 222, Subpart J)?
2. Has the financial institution adequately developed and maintained a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of new and existing accounts that are covered by the FACT Act?
3. Did the financial institution evaluate whether its Program includes reasonable policies and procedures to
   a. identify relevant Red Flags[1] for the financial institution's covered accounts and has it incorporated those Red Flags into its Program;

1. Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

   b. respond appropriately to prevent and mitigate identity theft detected by any Red Flags; and
   c. ensure that the Program is updated periodically to reflect changes in identity theft risks to customers and to the safety and soundness of the financial institution?
4. Has the Program included Red Flags from sources such as
   a. incidents that the financial institution has experienced;
   b. methods of identity theft that the financial institution has identified that reflects changes in identity theft risks; and
   c. applicable supervisory guidance?
5. Does the Program include relevant Red Flags from the following categories (see supplement A to appendix J):
   a. alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as a fraud detection services;
   b. the presentation of suspicious documents;
   c. the presentation of suspicious personal identifying information, such as a suspicious address change;
   d. the unusual use of, or other suspicious activity related to, a covered account; and
   e. notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor?
6. If the financial institution has established and maintained a required Program, has the institution's Program included the relevant and appropriate guidelines that are found in the Board's rule's appendix J (12 CFR 222, appendix J)?
7. Were the examples of factors in appendix J's guidelines considered initially, and periodically, to determine the relevancy and appropriateness of the Program's Red Flags, such as
   a. the types of accounts it offers or maintains;
   b. the methods it provides to open its covered accounts;
   c. the methods it provides to access its covered accounts;
   d. its previous experiences with identity theft; and
   e. changes in the financial institution's business arrangements, including its mergers, acquisitions, and joint ventures, and its alliances and service provider arrangements?
8. Does the Program's policies and procedures address the detection of Red Flags in connection with the financial institution's opening of covered accounts and existing covered accounts such as by
   a. obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
   b. authenticating customers, monitoring transactions; and verifying the validity of change of address requests?
9. If a required Program has been established by the financial institution, has it provided for the Program's continued administration by
   a. involving the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the continued oversight, development, implementation, and administration of the Program?
   b. training staff, as necessary, to effectively implement the Program?
   c. providing appropriate and effective oversight of its service provider arrangements?

CONCLUSION

1. Does the foregoing information constitute an adequate basis for evaluating internal control (that is, no significant deficiencies in areas not covered in this questionnaire impair any controls)? Explain negative answers briefly and indicate any additional examination procedures deemed necessary.
2. On the basis of a composite evaluation, as evidenced by answers to the foregoing questions, is internal control considered adequate or inadequate?

The Federal Reserve issued this guidance to assist financial institutions in understanding and managing the risks associated with outsourcing a bank activity to a service provider to perform that activity. Refer to SR-13-19/CA-13-21.

In addition to traditional core bank processing and information technology services, financial institutions[1] outsource operational activities such as accounting, appraisal management, internal audit, human resources, sales and marketing, loan review, asset and wealth management, procurement, and loan servicing. The Federal Reserve has issued this guidance to financial institutions to highlight the potential risks that arise from the use of service providers and to describe the elements of an appropriate service provider risk-management program. This guidance supplements existing guidance on technology service provider (TSP) risk,[2] and applies to service provider relationships where business functions or activities are outsourced. For purposes of this guidance, ''service providers'' is broadly defined to include all entities[3] that have entered into a contractual relationship with a financial institution to provide business functions or activities.

RISKS FROM THE USE OF SERVICE PROVIDERS

The use of service providers to perform operational functions presents various risks to financial institutions. Some risks are inherent to the outsourced activity itself, whereas others are introduced with the involvement of a service provider. If not managed effectively, the use of service providers may expose financial institutions to risks that can result in regulatory action, financial loss, litigation, and loss of reputation. Financial institutions should consider the following risks before entering into and while managing outsourcing arrangements.

- *Compliance risks* arise when the services, products, or activities of a service provider fail to comply with applicable U.S. laws and regulations.
- *Concentration risks* arise when outsourced services or products are provided by a limited number of service providers or are concentrated in limited geographic locations.
- *Reputational risks* arise when actions or poor performance of a service provider causes the public to form a negative opinion about a financial institution.
- *Country risks* arise when a financial institution engages a foreign-based service provider, exposing the institution to possible economic, social, and political conditions and events from the country where the provider is located.
- *Operational risks* arise when a service provider exposes a financial institution to losses due to inadequate or failed internal processes or systems or from external events and human error.
- *Legal risks* arise when a service provider exposes a financial institution to legal expenses and possible lawsuits.

BOARD OF DIRECTORS AND SENIOR MANAGEMENT RESPONSIBILITIES

The use of service providers does not relieve a financial institution's board of directors and senior management of their responsibility to ensure that outsourced activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations. Policies governing the use of service providers should be established and approved by the board of directors, or an executive committee of the board. These policies should establish a service provider risk management program that addresses risk assessments and due diligence, standards for contract provisions and considerations, ongoing monitoring of service providers, and business continuity and contingency planning.

Senior management is responsible for ensuring that board-approved policies for the use of service providers are appropriately executed. This includes overseeing the development and implementation of an appropriate risk-management and reporting framework that

1. For purposes of this guidance, a ''financial institution'' refers to state member banks, bank and savings and loan holding companies (including their nonbank subsidiaries), and U.S. operations of foreign banking organizations.

2. Refer to the FFIEC Outsourcing Technology Services Booklet (June 2004) at http://ithandbook.ffiec.gov/it-booklets/outsourcing-technology-services.aspx.

3. Entities may be a bank or nonbank, affiliated or non-affiliated, regulated or non-regulated, or domestic or foreign.

includes elements described in this guidance. Senior management is also responsible for regularly reporting to the board of directors on adherence to policies governing outsourcing arrangements.

SERVICE PROVIDER RISK-MANAGEMENT PROGRAMS

A financial institution's service provider risk-management program should be risk-focused and provide oversight and controls commensurate with the level of risk presented by the outsourcing arrangements in which the financial institution is engaged. It should focus on outsourced activities that have a substantial impact on a financial institution's financial condition; are critical to the institution's ongoing operations; involve sensitive customer information or new bank products or services; or pose material compliance risk.

The depth and formality of the service provider risk-management program will depend on the criticality, complexity, and number of material business activities being outsourced. A community banking organization may have critical business activities being outsourced, but the number may be few and to highly reputable service providers. Therefore, the risk-management program may be simpler and use less elements and considerations. For those financial institutions that may use hundreds or thousands of service providers for numerous business activities that have material risk, the financial institutions may find that they need to use many more elements and considerations of a service provider risk-management program to manage the higher level of risk and reliance on service providers.

While the activities necessary to implement an effective service provider risk-management program can vary based on the scope and nature of a financial institution's outsourced activities, effective programs usually include the following core elements:

- risk assessments, due diligence and selection of service providers;
- contract provisions and considerations;
- incentive compensation review;
- oversight and monitoring of service providers; and
- business continuity and contingency plans.

A. Risk Assessments

Risk assessment of a business activity and the implications of performing the activity in-house or having the activity performed by a service provider are fundamental to the decision of whether or not to outsource. A financial institution should determine whether outsourcing an activity is consistent with the strategic direction and overall business strategy of the organization. After that determination is made, a financial institution should analyze the benefits and risks of outsourcing the proposed activity as well as the service provider risk, and determine cost implications for establishing the outsourcing arrangement. Consideration should also be given to the availability of qualified and experienced service providers to perform the service on an ongoing basis. Additionally, management should consider the financial institution's ability and expertise to provide appropriate oversight and management of the relationship with the service provider.

This risk assessment should be updated at appropriate intervals consistent with the financial institution's service provider risk-management program. A financial institution should revise its risk mitigation plans, if appropriate, based on the results of the updated risk assessment.

B. Due Diligence and Selections of Service Providers

A financial institution should conduct an evaluation of and perform the necessary due diligence for a prospective service provider prior to engaging the service provider. The depth and formality of the due diligence performed will vary depending on the scope, complexity, and importance of the planned outsourcing arrangement, the financial institution's familiarity with prospective service providers, and the reputation and industry standing of the service provider. Throughout the due diligence process, financial institution technical experts and key stakeholders should be engaged in the review and approval process as needed. The overall due diligence process includes a review of the service provider with regard to business background, reputation, and strategy; financial performance and condition; and operations and internal controls.

1. Business Background, Reputation, and Strategy

Financial institutions should review a prospective service provider's status in the industry and corporate history and qualifications; review the background and reputation of the service provider and its principals; and ensure that the service provider has an appropriate background check program for its employees.

The service provider's experience in providing the proposed service should be evaluated in order to assess its qualifications and competencies to perform the service. The service provider's business model, including its business strategy and mission, service philosophy, quality initiatives, and organizational policies should be evaluated. Financial institutions should also consider the resiliency and adaptability of the service provider's business model as factors in assessing the future viability of the provider to perform services.

Financial institutions should check the service provider's references to ascertain its performance record, and verify any required licenses and certifications. Financial institutions should also verify whether there are any pending legal or regulatory compliance issues (for example, litigation, regulatory actions, or complaints) that are associated with the prospective service provider and its principals.

2. Financial Performance and Condition

Financial institutions should review the financial condition of the service provider and its closely related affiliates. The financial review may include:

- The service provider's most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity, and operating results.
- The service provider's sustainability, including factors such as the length of time that the service provider has been in business and the service provider's growth of market share for a given service.
- The potential impact of the financial institution's business relationship on the service provider's financial condition.
- The service provider's commitment (both in terms of financial and staff resources) to provide the contracted services to the financial institution for the duration of the contract.
- The adequacy of the service provider's insurance coverage.
- The adequacy of the service provider's review of the financial condition of any subcontractors.
- Other current issues the service provider may be facing that could affect future financial performance.

3. Operations and Internal Controls

Financial institutions are responsible for ensuring that services provided by service providers comply with applicable laws and regulations and are consistent with safe-and-sound banking practices. Financial institutions should evaluate the adequacy of standards, policies, and procedures. Depending on the characteristics of the outsourced activity, some or all of the following may need to be reviewed:

1. internal controls;
2. facilities management (such as access requirements or sharing of facilities);
3. training, including compliance training for staff;
4. security of systems (for example, data and equipment);
5. privacy protection of the financial institution's confidential information;
6. maintenance and retention of records;
7. business resumption and contingency planning;
8. systems development and maintenance;
9. service support and delivery;
10. employee background checks; and
11. adherence to applicable laws, regulations, and supervisory guidance.

C. Contract Provisions and Considerations

Financial institutions should understand the service contract and legal issues associated with proposed outsourcing arrangements. The terms of service agreements should be defined in written contracts that have been reviewed by the financial institution's legal counsel prior to execution. The characteristics of the business activity being outsourced and the service provider's strategy for providing those services will determine the terms of the contract. Elements of

well-defined contracts and service agreements usually include:

1. *Scope:* Contracts should clearly define the rights and responsibilities of each party, including:
   - support, maintenance, and customer service;
   - contract timeframes;
   - compliance with applicable laws, regulations, and regulatory guidance;
   - training of financial institution employees;
   - the ability to subcontract services;
   - the distribution of any required statements or disclosures to the financial institution's customers;
   - insurance coverage requirements; and
   - terms governing the use of the financial institution's property, equipment, and staff.
2. *Cost and compensation:* Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider. In addition, financial institutions should ensure that any incentives (for example, in the form of variable charges, such as fees and/or commissions) provided in contracts do not provide potential incentives to take imprudent risks on behalf of the institution.
3. *Right to audit:* Agreements may provide for the right of the institution or its representatives to audit the service provider and/or to have access to audit reports. Agreements should define the types of audit reports the financial institution will receive and the frequency of the audits and reports.
4. *Establishment and monitoring of performance standards:* Agreements should define measurable performance standards for the services or products being provided.
5. *Confidentiality and security of information:* Consistent with applicable laws, regulations, and supervisory guidance, service providers should ensure the security and confidentiality of both the financial institution's confidential information and the financial institution's customer information. Information security measures for outsourced functions should be viewed as if the activity were being performed by the financial institution and afforded the same protections. Financial institutions have a responsibility to ensure service providers take appropriate measures designed to meet the objectives of the information security guidelines within Federal Financial Institutions Examination Council (FFIEC) guidance,[4] as well as comply with section 501(b) of the Gramm-Leach-Bliley Act. These measures should be mapped directly to the security processes at financial institutions, as well as be included or referenced in agreements between financial institutions and service providers.

   Service agreements should also address service provider use of financial institution information and its customer information. Information made available to the service provider should be limited to what is needed to provide the contracted services. Service providers may reveal confidential supervisory information only to the extent authorized under applicable laws and regulations.[5]

   If service providers handle any of the financial institution customer's Nonpublic Personal Information (NPPI), the service providers must comply with applicable privacy laws and regulations.[6] Financial institutions should require notification from service providers of any breaches involving the disclosure of NPPI data. Generally, NPPI data is any nonpublic personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available.[7] Financial institutions and their service providers who maintain, store, or process NPPI data are responsible

4. For further guidance regarding vendor security practices, refer to the FFIEC Information Security Booklet (July 2006) at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx.
5. See 12 CFR Part 261.
6. See 12 CFR 1016.
7. See 12 USC 6801(b).

for that information and any disclosure of it. The security of, retention of, and access to NPPI data should be addressed in any contracts with service providers.

When a breach or compromise of NPPI data occurs, financial institutions have legal requirements that vary by state and these requirements should be made part of the contracts between the financial institution and any service provider that provides storage, processing, or transmission of NPPI data. Misuse or unauthorized disclosure of confidential customer data by service providers may expose financial institutions to liability or action by a federal or state regulatory agency. Contracts should clearly authorize and disclose the roles and responsibilities of financial institutions and service providers regarding NPPI data.

6. *Ownership and license:* Agreements should define the ability and circumstances under which service providers may use financial institution property inclusive of data, hardware, software, and intellectual property. Agreements should address the ownership and control of any information generated by service providers. If financial institutions purchase software from service providers, escrow agreements may be needed to ensure that financial institutions have the ability to access the source code and programs under certain conditions.[8]
7. *Indemnification:* Agreements should provide for service provider indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.
8. *Default and termination:* Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Agreements should also define termination rights, including change in control, merger or acquisition, increase in fees, failure to meet performance standards, failure to fulfill the contractual obligations, failure to provide required notices, and failure to prevent violations of law, bankruptcy, closure, or insolvency. Contracts should include termination and notification requirements that provide financial institutions with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of financial institution data, records, and other resources.
9. *Dispute resolution:* Agreements should include a dispute resolution process in order to expedite problem resolution and address the continuation of the arrangement between the parties during the dispute resolution period.
10. *Limits on liability:* Service providers may want to contractually limit their liability. The board of directors and senior management of a financial institution should determine whether the proposed limitations are reasonable when compared to the risks to the institution if a service provider fails to perform.[9]
11. *Insurance:* Service providers should have adequate insurance and provide financial institutions with proof of insurance. Further, service providers should notify financial institutions when there is a material change in their insurance coverage.
12. *Customer complaints:* Agreements should specify the responsibilities of financial institutions and service providers related to responding to customer complaints. If service providers are responsible for customer complaint resolution, agreements should provide for summary reports to the financial institutions that track the status and resolution of complaints.
13. *Business resumption and contingency plan of the service provider:* Agreements should address the continuation of services provided by service providers in the event of operational failures. Agreements should address service provider responsibility for backing up information and maintaining disaster recovery and contingency plans. Agreements may include a service provider's responsibility for testing of plans and providing testing results to financial institutions.
14. *Foreign-based service providers:* For agreements with foreign-based service providers,

8. Escrow agreements are established with vendors when buying or leasing products that have underlying proprietary software. In such agreements, an organization can only access the source program code under specific conditions, such as discontinued product support or financial insolvency of the vendor.

9. Refer to SR-06-4, "Interagency Advisory on the Unsafe and Unsound Use of Limitations on Liability Provisions in External Audit Engagement Letters," regarding restrictions on the liability limitations for external audit engagements or the manual's section 1010.1.

financial institutions should consider including express choice of law and jurisdictional provisions that would provide for the adjudication of all disputes between the two parties under the laws of a single, specific jurisdiction. Such agreements may be subject to the interpretation of foreign courts relying on local laws. Foreign law may differ from U.S. law in the enforcement of contracts. As a result, financial institutions should seek legal advice regarding the enforceability of all aspects of proposed contracts with foreign-based service providers and the other legal ramifications of such arrangements.

15. *Subcontracting:* If agreements allow for subcontracting, the same contractual provisions should apply to the subcontractor. Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Financial institutions should pay special attention to any foreign subcontractors, as information security and data privacy standards may be different in other jurisdictions. Additionally, agreements should include the service provider's process for assessing the subcontractor's financial condition to fulfill contractual obligations.

D. Incentive Compensation Review

Financial institutions should also ensure that an effective process is in place to review and approve any incentive compensation that may be embedded in service provider contracts, including a review of whether existing governance and controls are adequate in light of risks arising from incentive compensation arrangements. As the service provider represents the institution by selling products or services on its behalf, the institution should consider whether the incentives provided might encourage the service provider to take imprudent risks. Inappropriately structured incentives may result in reputational damage, increased litigation, or other risks to the financial institution. An example of an inappropriate incentive would be one where variable fees or commissions encourage the service provider to direct customers to products with higher profit margins without due consideration of whether such products are suitable for the customer.

E. Oversight and Monitoring of Service Providers

To effectively monitor contractual requirements, financial institutions should establish acceptable performance metrics that the business line or relationship management determines to be indicative of acceptable performance levels. Financial institutions should ensure that personnel with oversight and management responsibilities for service providers have the appropriate level of expertise and stature to manage the outsourcing arrangement. The oversight process, including the level and frequency of management reporting, should be risk-focused. Higher risk service providers may require more frequent assessment and monitoring and may require financial institutions to designate individuals or a group as a point of contact for those service providers. Financial institutions should tailor and implement risk mitigation plans for higher risk service providers that may include processes such as additional reporting by the service provider or heightened monitoring by the financial institution. Further, more frequent and stringent monitoring is necessary for service providers that exhibit performance, financial, compliance, or control concerns. For lower risk service providers, the level of monitoring can be lessened.

Financial condition: Financial institutions should have established procedures to monitor the financial condition of service providers to evaluate their ongoing viability. In performing these assessments, financial institutions should review the most recent financial statements and annual report with regard to outstanding commitments, capital strength, liquidity, and operating results. If a service provider relies significantly on subcontractors to provide services to financial institutions, then the service provider's controls and due diligence regarding the subcontractors should also be reviewed.

Internal controls: For significant service pro-

vider relationships, financial institutions should assess the adequacy of the provider's control environment. Assessments should include reviewing available audits or reports such as the American Institute of Certified Public Accountants' Service Organization Control 2 report.[10] If the service provider delivers information technology services, the financial institution can request the FFIEC Technology Service Provider examination report from its primary federal regulator. Security incidents at the service provider may also necessitate the institution to elevate its monitoring of the service provider.

Escalation of oversight activities: Financial institutions should ensure that risk-management processes include triggers to escalate oversight and monitoring when service providers are failing to meet performance, compliance, control, or viability expectations. These procedures should include more frequent and stringent monitoring and follow-up on identified issues, on-site control reviews, and when an institution should exercise its right to audit a service provider's adherence to the terms of the agreement. Financial institutions should develop criteria for engaging alternative outsourcing arrangements and terminating the service provider contract in the event that identified issues are not adequately addressed in a timely manner.

F. Business Continuity and Contingency Considerations

Various events may affect a service provider's ability to provide contracted services. For example, services could be disrupted by a provider's performance failure, operational disruption, financial difficulty, or failure of business continuity and contingency plans during operational disruptions or natural disasters. Financial institution contingency plans should focus on critical services provided by service providers and consider alternative arrangements in the event that a service provider is unable to perform.[11] When preparing contingency plans, financial institutions should

- ensure that a disaster recovery and business continuity plan exists with regard to the contracted services and products;
- assess the adequacy and effectiveness of a service provider's disaster recovery and business continuity plan and its alignment to their own plan;
- document the roles and responsibilities for maintaining and testing the service provider's business continuity and contingency plans;
- test the service provider's business continuity and contingency plans on a periodic basis to ensure adequacy and effectiveness; and
- maintain an exit strategy, including a pool of comparable service providers, in the event that a contracted service provider is unable to perform.

G. Additional Risk Considerations

Suspicious Activity Report (SAR) reporting functions: The confidentiality of suspicious activity reporting makes the outsourcing of any SAR-related function more complex. Financial institutions need to identify and monitor the risks associated with using service providers to perform certain suspicious activity reporting functions in compliance with the Bank Secrecy Act (BSA). Financial institution management should ensure they understand the risks associated with such an arrangement and any BSA-specific guidance in this area.

Foreign-based service providers: Financial institutions should ensure that foreign-based service providers are in compliance with applicable U.S. laws, regulations, and regulatory guidance. Financial institutions may also want to consider laws and regulations of the foreign-based provider's country or regulatory authority regarding the financial institution's ability to perform on-site review of the service provider's operations. In addition, financial institutions should consider the authority or ability of home country supervisors to gain access to the financial institution's customer information while examining the foreign-based service provider.

Internal audit: Financial institutions should refer to existing guidance on the engagement of independent public accounting firms and other outside professionals to perform work that has been traditionally carried out by internal

10. Refer to www.AICPA.org.

11. For further guidance regarding business continuity planning with service providers, refer to the FFIEC Business Continuity Booklet (March 2008) at http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning.aspx.

auditors.[12] The Sarbanes-Oxley Act of 2002 specifically prohibits a registered public accounting firm from performing certain non-audit services for a public company client for whom it performs financial statement audits.

Risk-management activities: Financial institutions may outsource various risk-management activities, such as aspects of interest rate risk and model risk management. Financial institutions should require service providers to provide information that demonstrates developmental evidence explaining the product components, design, and intended use, to determine whether the products and/or services are appropriate for the institution's exposures and risks.[13] Financial institutions should also have standards and processes in place for ensuring that service providers offering model risk-management services, such as validation, do so in a way that is consistent with existing model risk-management guidance.

12. Refer to SR-13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," specifically the section titled, "Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act." Refer also to SR-03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing," particularly the section titled,"Institutions Not Subject to Section 36 of the FDI Act that are Neither Public Companies nor Subsidiaries of Public Companies." See section 1010.1 of this manual.

13. Refer to SR-11-7, "Guidance on Model Risk Management," or section 4027.1, which informs financial institutions of the importance and risk to the use of models and the supervisory expectations that financial institutions should adhere to.

Electronic and Internet banking products and services have been widely adopted by financial institutions and are now a regular component of the business strategies at most institutions. Electronic and Internet delivery of services can have many far-reaching benefits for financial institutions and their customers. In some cases, however, these activities can have implications for a financial institution's financial condition, risk profile, and operating performance.

EXAMINATION APPROACH

In general, examiners should review electronic and Internet banking activities when these services are newly implemented, particularly in institutions that may not have significant experience or expertise in this area or when an institution is conducting novel activities that may pose a heightened risk. Periodic reviews should be conducted thereafter based on any significant changes to the scope of services or nature of the operations, as indicated by an assessment of risk to the institution.

Clearly, electronic and Internet banking concerns could affect an institution's operational-risk profile. Yet, these activities could also affect other financial and business risks, depending on the specific circumstances. Accordingly, examiners should consider an institution's electronic and Internet banking activities when developing risk assessments and supervisory plans. Although electronic and Internet banking may be assessed within the context of an information technology review, the nontechnical aspects of an electronic banking operation should be reviewed and coordinated closely with other examination areas. Rather than conduct detailed technical reviews, examiners should assess the overall level of risk any electronic and Internet banking activities pose to the institution and the adequacy of its approach to managing these risks.

To determine the scope of supervisory activities, close coordination is needed with information technology specialist examiners and consumer compliance examiners during the risk-assessment and planning phase, as well as during on-site examinations. Given the variability of electronic and Internet banking environments, the level of technical expertise required for a particular examination will differ across institutions and should be identified during the planning phase of the examination. When the bank has developed the electronic and Internet banking products or services internally or when a direct connection exists between the institution's electronic and Internet banking systems and its core data processing system, consideration should be given to involving an information technology specialist examiner in the on-site review. The determination of the examination scope should be based on factors such as the following:

- implementation of significant new electronic banking products and services since the last examination
- significant changes in the composition or level of customers, earnings, assets, or liabilities generated or affected by the electronic banking activities
- new or significantly modified systems or outsourcing relationships for activities related to electronic banking
- the need for targeted examinations of business lines that rely heavily on the electronic banking systems or activities
- other potential problems or concerns that may have arisen since the last examination or the need to follow up on previous examination or audit issues

Many resources are available to examiners for reviewing electronic and Internet banking activities. In addition to the procedures in this section, further information can be found in section 4060.1, "Information Technology," and in the *Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook.* Other federal banking agencies have issued examination guidance relating to electronic and Internet banking, information technology, and information security that may be helpful to examiners in reviewing electronic banking activities. Consumer compliance issues are not addressed in this section.[1]

1. See the Federal Reserve regulations, FFIEC, and other interagency supervisory guidance. See also the FFIEC's "Guidance on Electronic Financial Services and Consumer Compliance" (July 15, 1998), for further information regarding compliance with consumer laws and regulations.

OVERVIEW OF ELECTRONIC BANKING SERVICES

Types of Services

Electronic banking services (including Internet banking services) are designed to provide banking customers with the capability to conduct banking business remotely through personal computers and other electronic devices. Electronic banking comprises personal computer (PC) banking through traditional proprietary communication channels; retail and corporate Internet banking services; telephone banking; and, potentially, other forms of remote electronic access to banking services.

Both large and small institutions offer a variety of Internet-based financial services. Many financial institutions are using the Internet to enhance their service offerings to existing customers. Other organizations may choose to expand their customer base to a wider geographic area by accepting online applications for loan and deposit products. A very small number of banking organizations are focusing on the Internet as their primary delivery channel, whether or not they maintain physical branches.

Current electronic banking products and services typically allow customers to obtain information on bank products and services through the bank's Internet web sites, apply online for new products and services, view loan- and deposit-account balances and transactions, transfer funds between accounts, and perform other banking functions. Most electronic banking services operate using standard Internet browser software installed on the customer's personal computer and do not require that the customer have any additional software or hardware. While electronic banking services have been oriented toward retail customers, many banking organizations offer small-business applications and corporate cash-management services through the Internet. These services typically include payroll, automated clearinghouse (ACH), and wire transfers. Wholesale banking services, which have been conducted electronically for many years, are also beginning to move from proprietary networks and communications channels to the Internet.

Information-only web sites provide the most basic and common form of electronic banking service. Most institutions contract with an Internet service provider (ISP) to provide Internet access and "host," or maintain and operate, the institution's web site. In some cases, the web site is maintained on the institution's own computers (web servers). Even if access to account information is not possible through the web site, institutions may receive e-mail inquiries from customers through their web site.

Transactional Internet banking sites allow customers to obtain online access to their account information and initiate transactions over the Internet. With most Internet banking services, the customer interacts with a stand-alone Internet banking system that has been preloaded with the customer's account balances, transaction history, and other information. Transactions initiated through the Internet banking system are processed by a separate Internet banking application and periodically posted to the institution's general ledger, deposit, and loan accounting systems. Interface or connection with the financial institution's core data processing and accounting systems typically occurs through either (1) a direct connection to the core processing system over a network or (2) a manual download or transfer of transaction data to a diskette or other portable media, which is then uploaded or sent to the core processing system. Most standardized Internet banking software packages now available have been designed with standard interfaces between Internet banking systems and common core-processing systems and software.

Electronic bill-payment services are typically provided to customers as part of most standard electronic banking services. These services generally include capabilities to pay any third party the customer designates, as well as pay companies designated for routine bill payments, such as utilities and credit card issuers. Electronic bill-presentment services, which are much less common, involve the electronic transmission of billing statements to the customer through e-mail or a web site, for subsequent payment through the electronic banking service.

Telephone banking, a fairly conventional form of electronic banking, is provided by many institutions. Telephone banking services generally allow customers to check account balances and transactions and to pay bills through touch-tone or voice-response systems. Banking organizations also offer consumer products and services through wireless devices, such as cellular telephones, pagers, personal digital assistants, handheld computers, or other devices that can

provide wireless access to an institution's services, either directly or through the Internet. Account aggregation is a web-based service offered by some financial institutions that consolidates customer-account information from multiple financial or commercial web sites and presents it on a single web site. Aggregated information may include information from financial and nonfinancial accounts held by the customer. Some institutions have established "portals," web sites that link customers to a variety of third-party sites, and alliances with other companies to provide banking or nonbanking services.

Operations

There are a variety of operational methods for providing electronic banking services. Banking organizations may perform their core data processing internally but outsource the Internet banking activities to a different vendor or service provider. A dedicated workstation at the financial institution is often used to transmit transaction data files between the institution's core processing system and the Internet application; the workstation also allows the financial institution to update parameters and perform other maintenance. Alternatively, the service provider for Internet banking may interface directly with the bank's core-processing service provider, if that function is also outsourced. In addition, many banking organizations purchase Internet banking services from their primary core-processing service provider, eliminating the need for external data transmissions. Even with this last structure, the institution maintains a local workstation to provide access to customer information or perform other administrative and maintenance functions for the Internet banking system.

Other institutions operate an electronic banking system in their own computer facilities by purchasing an "off-the-shelf" or turnkey electronic banking software application from a software vendor and then installing the software on their own system. Turnkey options vary from a bank's purchase and use of templates or modules, in which the bank chooses from a selection of standard services, to more complex situations in which the software vendor designs and develops the electronic banking software application to the bank's specifications. Turnkey vendors often provide hardware, software, and ongoing system service and maintenance.

Bill-payment processing is generally conducted through a specialized third-party processor. The payment processor receives payment instructions from the financial institution or the Internet banking service provider, initiates an ACH debit to the account of the customer, and credits the account of the payee. Payments to payees not set up to receive ACH payments, such as individuals and smaller companies, are transmitted by mailing a paper check to the payee.

RISK MANAGEMENT

Board and Management Oversight

Financial institutions commonly implement electronic banking services as a means of delivering existing banking products and services to existing customers. As a result, not all institutions have established a distinct risk-management program for electronic banking. In many cases, policies and procedures for electronic banking activities will be incorporated into existing policies and procedures, such as those governing deposit accounts, payments processing, information security, and lending functions.

Bank management should assess the financial impact of the implementation and ongoing maintenance of electronic banking services. For example, ongoing maintenance and marketing costs of Internet banking operations can be substantial, particularly for smaller banks, depending on the institution's business plan. Bank management should consider the potential impact on the institution's customer base, loan quality and composition, deposit volume, volatility, liquidity sources, and transaction volume, as well as the impact on other relevant factors that may be affected by the adoption of new delivery channels. These areas should be monitored and analyzed on an ongoing basis to ensure that any impact on the institution's financial condition resulting from electronic banking services is appropriately managed and controlled.

In addition, bank management may wish to review periodic reports tracking customer usage, problems such as complaints and downtime, unreconciled accounts or transactions initiated through the electronic banking system, and system usage relative to capacity. Management

should also consider the expertise of internal or external auditors to review electronic banking activities and the inclusion of electronic banking activities within audit plans. Insurance policies may need to be updated or expanded to cover losses due to system security breaches, system downtime, or other risks from electronic banking activities.[2]

A change in an institution's business strategy to an Internet-only or Internet-focused operation is generally considered a significant change in business plan.[3] In addition, certain technology operations, such as providing ISP services to the general public, may not be considered permissible banking activities or may be considered permissible by the institution's chartering authority only within certain limitations.

A financial institution should also consider legal ownership of its Internet address (for example, www.bankname.com), also known as its "domain name." Contracts with third-party vendors may specifically address any arrangements to have the third-party vendor register the domain name on behalf of the institution.

Operational and Internal Controls

Web Site Information Maintenance

Because an institution's web site is available on an ongoing basis to the general public, appropriate procedures should be established to ensure the accuracy and appropriateness of its information. Key information changes and updates, such as loan rates, are normally subject to documented authorization and dual verification. Establishing procedures and controls to frequently monitor and verify web site information may help prevent any inadvertent or unauthorized modifications or content, which could lead to reputational damage or violations of advertising, disclosure, or other compliance requirements.

In addition, some institutions provide financial-calculator, financial-management, tax-preparation, and other interactive programs to customers. Institutions may provide online resources for customers to research available options associated with savings products, mortgages, investments, insurance, or other products and services. To protect the institution from potential liability or reputational harm, the bank should test or otherwise verify the accuracy and appropriateness of these tools.

Banks should carefully consider how links to third-party Internet web sites are presented. Hyperlinks to other web pages provide customers with convenient access to related or local information, as well as provide a means for targeted cross-marketing through agreements between the institution and other web site operators. However, such linkages may imply an endorsement of third-party products, services, or information that could lead to implicit liability for the institution. As a result, institutions commonly provide disclaimers when such links take the customer to a third-party web site. Institutions should ensure that they clearly understand any potential liabilities arising out of any cross-marketing arrangements or other agreements with third parties. Any links to sites offering nondeposit investment or insurance products must comply with relevant interagency guidelines.[4] Links to other sites should be verified regularly for their accuracy, functionality, and appropriateness.

Customer Authentication in an Electronic Banking Environment and Administrative Controls

Customer authentication guidance issuances. The federal banking agencies have issued various iterations of examination guidance on authentication in an Internet banking environment to assist examiners with this evolving issue. On August 8, 2001, the FFIEC initially released "Authentication in an Electronic Banking Environment," which reviewed the risks and risk-management controls of authentication tools used to verify the identity of new cus-

2. See section 4040.1, "Management of Insurable Risks," for further information about fraud and computer-related insurance that may be applicable to electronic banking activities.

3. Regulation H sets forth the requirements for membership of state-chartered banks in the Federal Reserve System and imposes certain conditions of membership on applicant banks. A member bank must "at all times conduct its business and exercise its powers with due regard to safety and soundness" and "may not, without the permission of the Board, cause or permit any change in the general character of its business or in the scope of the corporate powers it exercises at the time of admission to membership" (12 CFR 208.3(d)(1) and (2)).

4. See section 4170.3, "Examination Procedures—Retail Sales of Nondeposit Investment Products," and the consumer protection rules for sales of insurance (65 *Fed. Reg.* 75,822 (December 4, 2000)).

tomers and authenticate existing customers. In response to significant legal and technological changes, the FFIEC issued a similarly titled statement on October 12, 2005, which replaced the 2001 guidance. As discussed in this section, the 2005 guidance addressed the need for risk-based assessments, customer awareness, and enhanced security measures to authenticate customers using Internet-based products and services that process high-risk transactions involving access to customer information or the movement of funds to other parties. One of the key points of emphasis of the guidance was that single-factor authentication, as the only control mechanism, is inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. (See SR-05-19.) To assist the banking industry and examiners, the Board, the FFIEC, and the other federal banking and thrift agencies issued frequently asked questions (FAQs) on August 15, 2006. (See SR-06-13.) The FAQs are designed to assist the financial institutions and their technology service providers in conforming to the guidance by addressing common questions on the scope, risk assessments, timing, and other issues.

On June 29, 2011, the FFIEC released "Supplement to Authentication in an Internet Banking Environment." (See SR-11-9.) The purpose of the 2011 supplement is to reinforce the existing guidance on risk-management framework and update the agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment. The supplement establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in certain situations.

Customer authentication background. Authentication describes the process of verifying the identity of a person or entity. The authentication process is one method used to control access to customer accounts and personal information, and is dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity. Many banks use the same account-opening procedures for electronic applications as they do for mailed or in-person applications. Procedures for accepting electronic account applications generally address areas such as—

- the type of funding accepted for initial deposits;
- funds-availability policies for deposits in new accounts;
- the timing of account-number, check, and ATM-card issuance;
- the minimum customer information required to open new accounts;
- single-factor, tiered single-factor, and multifactor authentication procedures for verification of information provided by the applicant (for example, verifying customer information against credit bureau reports); and
- screening for prior fraudulent account activity, typically using fraud-detection databases.[5]

Strong customer-authentication practices are necessary to help institutions detect and reduce fraud, detect and reduce identity theft, and enforce anti-money-laundering measures. Customer interaction with institutions continues to migrate from physical recognition and paper-based documentation to remote electronic access and transaction initiation. Significant risks potentially arise when an institution accepts new customers through the Internet or other purely electronic channels because of the absence of the physical cues that bankers traditionally use to identify individuals. The risks of doing business with unauthorized or incorrectly identified individuals in an electronic banking environment could result in financial loss and reputation damage.

In addition to limiting unauthorized access, effective authentication provides institutions with the appropriate foundation for electronic agreements and transactions. First, effective authentication provides the basis for the validation of parties to the transaction and their agreement to its terms. Second, authentication is a necessary element to establish the *authenticity* of the records evidencing the electronic transaction if there is ever a dispute. Third, authentication is a necessary element for establishing the *integrity* of the records evidencing the electronic transaction. Because state laws vary, management should involve legal counsel in the design and implementation of authentication systems.

The success of a particular authentication method depends on more than the technology.

5. For information on practices that my help prevent fraudulent account activity, see SR-01-11, "Identity Theft and Pretext Calling."

Success also depends on an institution's having appropriate policies, procedures, and controls. An effective authentication method has the following characteristics: customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans. The June 29, 2011, "Supplement to Authentication in an Internet Banking Environment" discusses the effectiveness of certain authentication techniques, namely device identification and the use of challenge questions.

Institutions can use a variety of authentication tools and methodologies to authenticate customers. These tools include the use of passwords and personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards or other types of "tokens," database comparisons, and biometric identifiers. The level of risk protection afforded by each of these tools varies and is evolving as technology changes.

Existing authentication methodologies involve three basic "factors":

- something the user *knows* (a password or PIN)
- something the user *possesses* (an ATM card or a smart card)
- something the user *is* (a biometric characteristic, such as a fingerprint or retinal pattern)

Authentication methods that depend on more than one factor typically are more difficult to compromise than single-factor systems. Accordingly, properly designed and implemented multifactor authentication methods are more reliable indicators of authentication and are stronger fraud deterrents. For example, the use of a log-on ID or password is single-factor authentication (something the user knows), whereas a transaction using an ATM typically requires two-factor authentication (something the user possesses—the card—combined with something the user knows—the PIN). In general, multifactor authentication methods should be used on higher-risk systems. Further, institutions should be sensitive to the fact that proper implementation is key to the reliability and security of any authentication system. For example, a poorly implemented two-factor system may be less secure than a properly implemented single-factor system.

Risk assessment. An effective authentication program should be implemented on an enterprise-wide basis to ensure that controls and authentication tools are adequate among all products, services, and lines of business. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for electronic banking and e-commerce customer services. The level of authentication a financial institution uses in a particular application should be appropriate to the level of risk in that application.

The implementation of appropriate authentication methods starts with an assessment of the risk posed by the institution's electronic banking systems. The risk-assessment process should

- identify all transactions and levels of access associated with Internet-based customer products and services;
- identify and assess the risk-mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and
- include the ability to gauge the effectiveness of risk-mitigation techniques for current and changing risk factors for each transaction type and level of access.

The risk should be evaluated in light of the type of customer (retail or commercial), the institution's transactional capabilities (bill payment, wire transfer, or loan origination), the sensitivity and value of the stored information to both the institution and the customer, the ease of using the authentication method, and the size and volume of transactions.

For example, online retail transactions generally involve accessing account information, bill payment, intrabank funds transfers, and occasional interbank funds transfers or wire transfers. Since the frequency and dollar amounts of these transactions are generally lower than commercial transactions, they pose a comparatively lower level of risk. Online commercial transactions generally involve ACH file origination and frequent interbank wire transfers. Since the frequency and dollar amounts of these transactions are generally higher than consumer transactions, they pose a comparatively increased level of risk to the institution and its customer. As such, it is recommended that institutions offer multifactor authentication to their business customers.

The Federal Reserve expects financial institutions to assess the risks to the institution and

its customers and to implement appropriate authentication methods to effectively manage risk. Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every 12 months. (See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Risk Assessment Practices section.) Updated risk assessments should consider, but not be limited to, the following factors:

- changes in the internal and external threat environment (see the attachment to SR 11-9 for more information)
- changes in the customer base adopting electronic banking
- changes in the customer functionality offered through electronic banking
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry

A comprehensive approach to authentication requires development of and adherence to corporate standards and architecture, integration of authentication processes within the overall information security framework, risk assessments within the institution's lines of business that support the selection of authentication tools, and a central authority for oversight and risk monitoring. The authentication process should be consistent and support the financial institution's overall security and risk-management programs.

The methods of authentication used in a specific electronic application should be appropriate and "reasonable," from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and service providers should periodically review authentication technology and ensure appropriate changes are implemented.

Single-factor authentication tools, including passwords and PINs, have been widely utilized in a variety of retail e-banking activities, including account inquiry, bill payment, and account aggregation. However, not every online transaction poses the same level of risk. Therefore, financial institutions should implement more robust controls as the risk level of the transaction increases. Financial institutions should assess the adequacy of existing authentication techniques in light of changing or new risks (for example, the increasing ability of hackers to compromise less robust single-factor techniques or the risks posed by phishing, pharming, or malware). Financial institutions should no longer rely on one form of customer authentication. A one-dimensional customer authentication program is simply not robust enough to provide the level of security that customers expect and that protects institutions from financial and reputation risk. Instead, multifactor techniques are appropriate for high-risk applications and transactions, which involve access to customer information or the movement of funds to other parties. Institutions should recognize that a single-factor system may be "tiered" to enhance security without implementing a two-factor system. A tiered single-factor authentication system would include the use of multiple levels of a single factor (for example, the use of two or more passwords or PINs employed at different points in the authentication process).

Account origination and customer verification. Institutions need to use reliable methods for originating new customer accounts online. Customer-identity verification during account origination is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. In an electronic banking environment, reliance on traditional forms of paper-based authentication is decreased substantially. Accordingly, financial institutions need to use reliable alternative methods. For example, verification of personal information could include the following:

- *Positive verification* to ensure that material information provided by an applicant matches information available from trusted third-party sources. More specifically, an institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (for example, a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the institution with an increasing level of confidence that the applicants are who they say they are.
- *Logical verification* to ensure that information provided is logically consistent. (For example,

do the telephone area code, ZIP code, and street address match?)

- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, however, a sole reliance on online electronic database comparison techniques is not adequate since certain documents needed to establish an individual's right to act on a company's behalf (for example, bylaws) are not available from databases. Institutions must still rely on traditional forms of personal identification and document validation combined with electronic verification tools.

Transaction initiation and authentication of established customers. Once an institution has successfully verified a customer's identity during the account-origination process, it should authenticate customers who wish to gain access to the online banking system. Institutions can use a variety of methods to authenticate existing customers. These methods include the use of passwords, PINs, digital certificates and a PKI, physical devices such as tokens, and biometrics.

Minimizing fraud risk. An institution's policies and procedures should address the management of existing customers' accounts to minimize the risk of fraudulent activity. For example, the customer's ability to expand an existing account relationship through the electronic banking system may warrant added controls, such as sending a separate notification to a customer's physical address when online account access is first requested or when PINs, e-mail addresses, or other key parameters are changed.

To mitigate fraud risk, institutions may establish dollar limits on transactions initiated through the electronic banking application, or they may monitor transactions above specified limits, depending on the type of account (for example, consumer versus corporate). These limits or a similar monitoring system may help detect unusual account activity, which could indicate fraudulent transactions or other suspicious activity.

Funds transfer systems and Internet banking. Any manual interface between the electronic banking system and funds transfer systems, such as capabilities for uploading ACH or Fedwire transactions initiated through the electronic banking system to Fedline terminals, should be subject to system-access controls and appropriate internal controls, such as segregation of duties. Some institutions also permit electronic banking customers to initiate electronic (ACH) debits against accounts held at other institutions; reliable controls to verify that the customer is entitled to draw funds from the particular account are needed if this feature is offered.

Electronic bill-payment services are commonly provided as a component of electronic banking services. The institution should have a direct agreement with bill-payment providers, which may be subcontractors of the provider for the institution's Internet banking services. In this situation, it may be difficult for the institution or its customers to obtain timely and accurate information regarding the status of payment requests. As a result, contracts with service providers that encompass bill-payment services should generally address how payments are made, when payments are debited from a customer account, the treatment of payments when the account has insufficient funds on the settlement date, reconcilement procedures, and problem-resolution procedures.

Even when Internet banking operations are outsourced to a service provider, institutions will generally have access to the electronic banking system through a dedicated desktop computer or workstation. This hardware allows the institution to upload and download transaction information; review transaction logs or audit trails; print daily reports; or, in some cases, reset customer passwords, resolve errors, or respond to customer inquiries. These workstations should be located in secure areas and be subject to normal authorization and access controls and transaction audit trails.

Information Security

Electronic banking activities should be addressed in an institution's information security program, which should include compliance with the federal banking agencies' information security standards.[6] Institutions

6. See section 4060.1 under "Standards for Safeguarding Customer Information" for further details and examination procedures. See also SR-01-25. See also the *FFIEC IT*

need to pay particular attention to the security of customer information, given the heightened security concerns associated with providing access to customer information over the Internet. An institution's written information security policies and procedures should include electronic banking activities. Institutions should implement prudent controls that limit the risk of unauthorized access to key systems, including password-administration controls, firewalls, encryption of sensitive information while it is in transit or being stored, maintenance of all current updates and security patches to software and operating systems, and controls to prevent insider misuse of information. Sound information security practices include procedures and systems to detect changes to software or files, intrusion-detection systems, and security-vulnerability assessments.

Sound information security practices are also based on the concept of layered security, which is the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Layered security can substantially strengthen the overall security of Internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses. Financial institutions should implement a layered approach to security for high-risk Internet-based systems. Other regulations and guidelines also specifically address financial institutions' responsibilities to protect customer information and prevent identity theft.[7]

Effective controls that may be included in a layered security program include, but are not limited to

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;
- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;
- enhanced controls over account activities, such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);
- Internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

At a minimum, an institution's layered security program should (1) detect and respond to suspicious activity and (2) control administrative functions. To detect and respond to suspicious activities, appropriate control processes should be instituted that detect anomalies and effectively respond to suspicious or anomalous activity related to initial login and authentication of customers requesting access to the institution's electronic banking system, as well as the initiation of electronic transactions involving the transfer of funds to other parties. Manual or automated transaction monitoring or anomaly detection and response may prevent instances of ACH/wire transfer fraud since fraudulent wire activities are typically anomalous when compared with the customer's established patterns of behavior.

A layered security program should also control administrative functions. For business accounts, layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. These enhanced controls should exceed the controls applicable to routine business customer users. For example, a preventive control could include requiring an additional authenti-

Examination Handbook, Information Security Booklet, July 2006, Key Concept section.

7. See Interagency Final Regulation Guidelines on Identity Theft Red Flags, 12 CFR parts 41, 222, 334, 571, and 717; Interagency Guidelines Establishing Information Security Standards, 12 CFR parts 30, 208, 225, 364, and 570, Appendix B. See also Section 4060.1 under "Identity Theft Red Flags Program" for further details and examination procedures.

cation routine or a transaction verification routine prior to final implementation of the access or application changes. An example of a detective control could include a transaction verification notice immediately following implementation of the submitted access or application changes. Out-of-band authentication, verification, or alerting can be effective controls. Overall, enhanced controls over administrative access and functions can effectively reduce money transfer fraud.

While the technical aspect of information security considerations for electronic banking activities is complex, widely used turnkey software applications for Internet banking generally conform to accepted industry standards for technical security. Detailed assessments of the technical security of specific systems are the responsibility of the institution and its qualified engineers and internal and external auditors. Examiners should focus on the institution's implementation of key security controls for the particular software application.

Any security breaches of an institution's electronic banking service or web site that may lead to potential financial losses or disclosure of sensitive information should be reported to an appropriate management level within the institution. If necessary, the appropriate suspicious-activity report should be filed. Institutions should ensure that their service providers notify them of any computer security breaches in their operations that may affect the institution. Institutions should determine the cause of any such intrusions and develop an appropriate plan to limit any resulting financial losses to the bank and its customers and to prevent recurrence.

Passwords and System-Access Controls

Most institutions use identifiers such as account numbers or ATM card numbers, together with passwords or PINs, to verify the authorization of users accessing the retail electronic banking system. (Wholesale or corporate cash-management systems may use more secure methods, such as smart cards that contain customer credentials, real-time passwords (passwords that can be immediately changed online), or dedicated terminals, to authenticate users.) Prudent password-administration procedures generally require that customer passwords be changed if compromised and that passwords do not automatically default to easily guessed numbers or names. Passwords and PINs are (1) generally encrypted while in transit or storage on insecure networks or computers, (2) suppressed on screen when entered on a keyboard, and (3) suspended after a predetermined number of failed log-in attempts. Institutions should establish clear policies and procedures for retrieving or resetting customer passwords when customers lose or forget their password to minimize the risk that passwords are disclosed to unauthorized individuals.[8]

Firewalls

A firewall is a security control consisting of hardware, software, and other security measures established to protect the bank's internal data and networks, as well as its web sites, from unauthorized external access and use through the Internet. A number of banks and their vendors use various firewall products that meet industry standards to secure their Internet banking services, web sites, and other bank networks. For a firewall to adequately protect a bank's internal networks and systems, it must be properly installed and configured. Firewalls are most effective when all updates and patches to the firewall systems are installed and when the firewall configuration is reassessed after every system change or software update.

Viruses

Computer viruses can pose a threat to information systems and networks that are connected to the Internet. In addition to destroying data and possibly causing system failure, viruses can potentially establish a communication link with an external network, allow unauthorized system access, or even initiate unauthorized data transmission. Widely used protection measures include using anti-virus products that are installed and are resident on a computer or network or providing for virus scanning during downloads of information or the execution of any program. Bank employees and electronic banking customers should be educated about the risks posed to systems by viruses and other malicious programs, as well as about the proper procedures for accessing information to help avoid these threats.

8. See SR-05-19 for further information on password-administration practices.

Encryption of Communications

Information transmitted over the Internet may be accessible to parties other than the sender and receiver. As a result, most retail electronic commerce services use industry-standard secure sockets layer (SSL) technology to encrypt sensitive transactional information between the customer and the web site to minimize the risk of unauthorized access to this information while it is in transit. Although stronger encryption techniques may be warranted for higher-value corporate or wholesale transactions, SSL is generally considered adequate for retail Internet banking transactions.

In addition, many banks accept communications through standard Internet e-mail; in some cases, account applications containing sensitive customer data may be sent to the bank. These communications are generally not protected by SSL or a similar technology but are open to potential unauthorized access. If the electronic banking system does not provide for encrypted e-mail, the bank should ensure that customers (and customer-service representatives) are alerted not to send confidential information by unencrypted e-mail.

Security Testing and Monitoring

Assessments of information security vulnerability, penetration testing, and monitoring help ensure that appropriate security precautions have been implemented and that system security configurations are appropriate. Some institutions contract with third-party security experts to provide these services. Vulnerability assessments provide an overall analysis of system security and report any system vulnerabilities. Such assessments can detect known security flaws in software and hardware, determine system susceptibility to known threats, and identify vulnerabilities such as settings that are contrary to established security policies.

Penetration testing and vulnerability assessments identify an information system's vulnerability to intrusion. Penetration tests examine system security by mimicking external intrusion attempts to circumvent the security features of a system. However, a penetration test is only a snapshot in time and does not guarantee that the system is secure.

Intrusion detection is an ongoing process that monitors the system for intrusions and unusual activities. Intrusion-detection systems, which can be installed on individual computers and at locations on a network, can be configured to alert appropriate system personnel to potential intrusions at the time they occur. In addition, the detection systems provide ongoing reporting and monitoring of unusual events such as potential intrusions or patterns of misuse.

Customer Awareness and Education

Because customer awareness is a key defense against fraud and identity theft, financial institutions should make efforts to educate their customers. Institutions should evaluate their consumer education efforts to determine if additional steps are necessary. The June 29, 2011, "Supplement to Authentication in an Internet Banking Environment" states that financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- an explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access
- an explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials
- a suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically
- a listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found
- a listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events

Contingency Planning

Periodic downtime and outages are common with online services. But when the duration or

disruption of these outages is significant, it can lead to reputational risk for the institution. For many institutions, short disruptions of electronic banking services may not have a material effect on their operations or customers, as other delivery channels are available. Nevertheless, electronic banking services should be covered by an institution's business-continuity plans. Institutions should assess their disaster-recovery needs by considering the length of time that electronic banking services could be unavailable to customers or for internal processing, and then design backup capabilities accordingly. In some cases, institutions may need to establish the capability to move processing to a different network or data center, or to move electronic banking services to a backup web site.

Typically, the electronic banking system includes capabilities to generate backup files on tapes, diskettes, or other portable electronic media containing key transaction and customer data. Web site information should also be subject to periodic backup. Security and internal controls at backup locations should be as sophisticated as those in place at the primary site. If a bank outsources electronic banking operations to a service provider, the institution should have a full understanding of the service provider's contingency and business-recovery commitments.[9]

Outsourcing Arrangements

Many institutions outsource electronic banking operations to an affiliate or third-party vendor. In addition to operating the Internet banking software application, service providers may provide services such as web site hosting and development, Internet access, and customer service or call-center maintenance. As with other areas of a bank's operations, examiners should evaluate the adequacy of the institution's oversight of its critical service providers.[10]

Banking organizations should consider requiring Internet banking service providers to obtain periodic security reviews performed by an independent party. The client institution should receive reports summarizing the findings.

9. For additional information on business resumption and contingency planning in relation to outsourcing, see section 4060.1, "Information Technology," and the *FFIEC Information Systems Examination Handbook*.

10. See section 4060.1, "Information Technology," and the *FFIEC Information Systems Examination Handbook* for information on risk management for outsourcing arrangements.

1. To develop an understanding of the significance of the bank's electronic banking activities within and across business lines.
2. To assess the types and levels of risks associated with the bank's electronic banking activities.
3. To exercise appropriate judgment when determining the level of review, given the characteristics, size, and business activities of the organization.
4. To assess the current and potential impact of electronic banking activities on the institution's financial profile and condition.
5. To assess the adequacy of risk management and oversight of electronic banking activities, including outsourced activities.
6. To determine if the institution is complying with other applicable laws, rules and regulations.
7. To prepare examination report comments on significant deficiencies and recommended corrective action.
8. To determine the impact, if any, of electronic banking risks on the CAMELS rating, information technology rating, and risk-management ratings.
9. To update the workpapers with any information that will facilitate future examinations.

1. Identify the bank's current and planned electronic banking activities and review the bank's public Internet web sites. Consider whether the bank provides the following types of services:
   a. telephone banking
   b. retail Internet banking services
   c. corporate or wholesale Internet banking services
   d. Internet service provider (ISP)
   e. brokerage services over the Internet
   f. insurance services over the Internet
   g. trust services over the Internet
   h. account aggregation
   i. electronic bill payment
   j. other activities (for example, web portals, financial calculators, cross-marketing arrangements and alliances, or unique services)
2. Review prior examination findings and workpapers related to electronic banking, including consumer compliance, information technology, and other examination areas that may be relevant.
3. Determine if material changes have been made to electronic banking products, services, or operations since the last examination and if any significant changes are planned in the near future.
   a. Ensure the bank has reviewed and updated the existing risk assessment prior to implementing new electronic financial services.
   b. If the bank has not materially changed its electronic banking services, determine if the board or senior management has reviewed the risk assessment within the past 12 months.
4. Determine the significance of the bank's electronic banking activities. Consider the following areas:
   a. approximate percentages and numbers of customers (for example, loan and deposit) that regularly use electronic banking products and services
   b. lending and deposit volumes generated from Internet applications
   c. the current monthly transaction and dollar volume for electronic banking services
   d. costs and fees to operate the system and related services or marketing programs
5. Incorporate an analysis of electronic banking activities into risk assessments, supervisory plans, and scope memoranda, considering the size, activities, and complexity of the organization, as well as the significance of the activities across particular business lines.
6. Assess the level of risk and the current or potential impact of electronic banking activities on the organization's earnings, liquidity, asset quality, operational risk, and consumer compliance. Communicate any concerns to examiners reviewing these areas.
7. Determine if the bank operates its web sites, electronic banking systems, or core data processing systems internally and whether any activities are outsourced to a vendor. If outsourced, all activities should be supported by written agreements that have been reviewed by the bank's legal counsel. Identify the location of the following operations:
   a. design and maintenance of the bank's public web site or home page
   b. computer or server for the bank's public web site
   c. development and maintenance of the bank's electronic banking systems
   d. computer or server for the bank's electronic banking systems
   e. customer service (for example, a call center) for electronic banking services
   f. electronic bill-payment processing or other ancillary services
8. If the bank operates the electronic banking system or core data processing system in-house, review the topology (schematic diagram) of the systems and networks, and determine whether there is a direct, online connection between the bank's core processing systems and the electronic banking system.
9. If the bank operates the electronic banking system or core data processing system in-house, review the transaction-processing flows between the electronic banking system and the bank's core processing systems and identify key control points. Determine whether information is exchanged in a real-time, batch (overnight), or hybrid-processing mode.

10. Review any available audits or third-party reviews of vendors or service providers the bank uses, such as Service Organization Control Reports (formerly SAS 70 reports).[1] Review any Federal Financial Institutions Examination Council (FFIEC) Shared Application Software Review (SASR) reports or any FFIEC or other supervisory examination reports of service providers that the institution uses.
11. Determine the adequacy of risk management for electronic banking activities (including authentication methods for prospective and existing customers), given the level of risk these activities pose to the institution.[2] Complete or update relevant portions of the electronic banking internal control questionnaire as needed for the specific electronic banking activities identified in the previous steps of these procedures to evaluate the adequacy of—
    a. policies and procedures governing electronic banking activities,
    b. internal controls and security for electronic banking activities,
    c. audit coverage for electronic banking activities,
    d. monitoring and compliance efforts,
    e. vendor and outsourcing management, and
    f. board and management oversight.
12. Determine if the bank engages in any "high-risk" transactions involving access to customer information or the movement of funds to other parties.
    a. If the bank engages in high-risk transactions, ensure the institution has implemented a layered security program and does not rely solely on any single control for authorizing such transactions.[3]
    b. Ensure the bank's layered security program is consistent with the risk for covered consumer and business (commercial) transactions.
13. Perform additional analysis and review, consulting with information technology specialists, consumer compliance specialists, or other subject-matter experts as needed, on areas of potential concern.
14. Determine the impact of any electronic banking activities or internal-control deficiencies on the financial condition of the organization.
15. Determine the extent of supervisory attention needed to ensure that any weaknesses are addressed and that associated risk is adequately managed.
16. Determine the impact of any deficiencies on the CAMELS rating, information technology rating, operational-risk rating, and any other relevant supervisory ratings.
17. Prepare comments for the examination report on any significant deficiencies and recommended corrective action.
18. Update the workpapers with any information that will facilitate future examinations.

1. Effective June 15, 2011, the Statement on Standards for Attestation Engagements (SSAE) No. 16, "Reporting on Controls at a Service Organization," replaces the guidance for service auditors in the American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) No. 70 "Service Organizations."

2. See SR-05-19, "FFIEC Guidance on Authentication in an Internet Banking Environment," and SR-11-19, "Interagency Supplement to Authentication in an Internet Banking Environment."

3. See SR-11-9 and Section 4063.1.

Electronic Banking
Internal Control Questionnaire
Effective date May 2007

Section 4063.4

Review the bank's internal controls, policies, practices, and procedures for electronic banking activities. Complete those questions necessary to assess whether any potential concerns warrant further review.

POLICIES AND PROCEDURES

1. Are updates and changes to the bank's public web sites—
   a. made only by authorized staff?
   b. subject to dual verification?
2. Are web site information and links to other web sites regularly verified and reviewed by the bank for—
   a. accuracy and functionality?
   b. potential reputational, compliance, and legal risk?
   c. appropriate disclaimers?
3. Do operating policies and procedures include—
   a. procedures for and controls over the opening of new customer accounts submitted through electronic channels in order to verify potential customer identity and financial condition?
   b. single-factor and tiered single-factor or multifactor procedures for authenticating the identity of prospective and existing customers when administering access to the electronic banking system (for example, customer passwords, personal identification numbers (PINs), or account numbers)?
   c. requirements for review of or controls over wire transfers or other large transfers initiated through the electronic banking system, to watch for potentially suspicious activity?
   d. appropriate authorizations for electronic debits initiated against accounts at other institutions, if such transfers are allowed?
   e. depending on the type of account, dollar limits on transactions over a given time period initiated through the electronic banking service?
   f. reconcilement and accounting controls over transactions initiated through the electronic banking system, including electronic bill-payment processing?
4. Do written information security policies and procedures address electronic banking products and services?
5. Are business-recovery procedures adequate? Do the procedures address—
   a. events that could affect the availability of the electronic banking system, such as system outages, natural disasters, or other disruptions?
   b. planned recovery times that are consistent with how important electronic banking activities are to the institution?
6. Has management established an adequate incident-response plan to handle and report potential system security breaches, web site disruptions, malicious tampering with the web site, or other problems?

AUDIT AND INDEPENDENT REVIEW

1. Do the bank's internal and external audit programs address electronic banking activities and systems?
2. Is the level of audit review commensurate with the risks in electronic banking activities and systems?
3. Do audits address—
   a. the review and testing of the bank's internal controls relating to electronic banking?
   b. the review of service-provider performance relative to contract terms, if services are outsourced?
   c. the review of the service providers' internal or external audits or third-party reviews, if services are outsourced?
4. Is management's response to any audit recommendations timely and appropriate?

INTERNAL CONTROLS AND SECURITY

1. Has the bank or service provider implemented a firewall to protect the bank's web site?
2. Are ongoing monitoring and maintenance arrangements for the firewall in place to ensure that it is properly maintained and configured?

3. If the bank uses a turnkey electronic banking software package or outsources to a service provider—
   a. are bank staff familiar with key controls detailed by the vendor's security and operating manuals and training materials?
   b. are workstations that interface with the service provider's system for administrative procedures or for the transfer of files and data kept in a secure location with appropriate password or other access control, dual-verification procedures, and other controls?
4. Does the bank's control of customer access to the electronic banking system include—
   a. procedures to ensure that only appropriate staff are authorized to access electronic banking systems and data, including access to any workstations connected to a remote system located at a service provider?
   b. levels of authentication methods that are commensurate with the level of risk in the bank's electronic banking applications?
   c. the length and composition of passwords and PINs?
   d. encryption of passwords and PINs in transit and storage?
   e. the number of unsuccessful log-on attempts before the password is suspended?
   f. procedures for resetting customer passwords and PINs?
   g. automatic log-off controls for user inactivity?
5. Have security-vulnerability assessments and penetration tests of electronic banking systems been conducted? Has the bank reviewed the results?
6. Has the bank or its service provider established—
   a. an intrusion-detection system for electronic banking applications?
   b. procedures to detect changes in electronic banking files and software?
   c. measures to protect the electronic banking system from computer viruses?
   d. procedures for ensuring on an ongoing basis that electronic banking applications, operating systems, and the related security infrastructure incorporate patches and upgrades that are issued to address known security vulnerabilities in these systems?
7. If e-mail is used to communicate with customers, are communications encrypted or does the bank advise customers not to send confidential information through e-mail?

MONITORING AND COMPLIANCE

1. Are adequate summary reports made available to management to allow for monitoring of—
   a. web site usage?
   b. transaction volume?
   c. system-problem logs?
   d. exceptions?
   e. unreconciled transactions?
   f. other customer or operational issues?
2. Has management established adequate procedures for monitoring and addressing customer problems with electronic banking products and services?
3. Does management accurately report its primary public web-site address on its Consolidated Report of Condition and Income?
4. Have required Suspicious Activity Reports involving electronic banking, including any computer intrusions, been filed? See the requirements for suspicious-activity reporting in section 208.62 of the Board's Regulation H (12 CFR 208.62), and the Bank Secrecy Act compliance program in section 208.63 (12 CFR 208.63).

VENDORS AND OUTSOURCING

1. Is each significant vendor, service provider, consultant, or contractor relationship that is involved in the development and maintenance of electronic banking services covered by a written, signed contract? Depending on the nature and criticality of the services, do contracts specify—
   a. minimum service levels and remedies or penalties for nonperformance?
   b. liability for failed, delayed, or erroneous transactions processed by the service provider and for other transactions in which losses may be incurred (for example, insufficient funds)?
   c. contingency plans, recovery times in the event of a disruption, and responsibility

for backup of programs and data?
   d. data ownership, data usage, and compliance with the bank's information security policies?
   e. bank access to the service provider's financial information and results of audits and security reviews?
   f. insurance to be maintained by the service provider?
2. Has legal counsel reviewed the contracts to ensure they are legally enforceable and that they reasonably protect the bank from risk?
3. Has the bank ensured that any service provider responsible for hosting or maintaining the bank's web site has implemented—
   a. controls to protect the bank's web site from unauthorized alteration and malicious attacks?
   b. procedures to notify the bank in the event of such incidents?
   c. regular backup of the bank's web site information?
4. Depending on the nature and criticality of the services, does the bank conduct initial and periodic due-diligence reviews of service providers, including—
   a. reviewing the service provider's standards, policies, and procedures relating to internal controls, security, and business contingency to ensure they meet the bank's minimum standards?
   b. monitoring performance relative to service-level agreements and communicating any deficiencies to the service provider and to bank management?
   c. reviewing reports provided by the service provider on response times, availability and downtime, exception reports, and capacity reports, and communicating any concerns to bank management and the vendor?
   d. periodically reviewing the financial condition of the service provider and determining whether backup arrangements are warranted as a result?
   e. reviewing third-party audits, SAS 70 reports, and regulatory examination reports on the service provider, if available, and following up on any findings with the service provider?
   f. conducting on-site audits of the service provider, if appropriate based on the level of risk?
   g. participating in user groups?
   h. ensuring the bank's staff receives adequate training and documentation from the vendor or service provider?
5. If the bank operates a turnkey electronic banking software package—
   a. is software held under an escrow agreement?
   b. has the bank established procedures to ensure that relevant program files and documentation held under the software escrow agreement are kept current and complete?
6. If a vendor maintains the bank's electronic banking system, does the bank monitor the on-site or remote access of its systems by the vendor, through activity logs or other measures?

BOARD AND MANAGEMENT OVERSIGHT

1. Does the board or an appropriate committee approve the introduction of new electronic banking products and services on the basis of a written business plan and risk analysis that are commensurate with the proposed planned activity?
2. Has the bank considered—
   a. whether the service is designed to provide information on existing services to existing customers or to attract new customers?
   b. whether financial incentives will be offered to attract customers through the electronic banking service? What is the financial impact of such incentives on the bank?
   c. the potential impact of electronic banking products and services on the composition of the bank's customer base?
   d. the projected financial impact of the new service, including up-front and operating costs and any impact on fees or other revenue or expenses?
   e. internal controls appropriate for the new product or service?
   f. whether adequate management reports are provided and subject to periodic review?
   g. whether any new nonbanking activities are permissible under applicable state and federal banking laws?
   h. the extent of outsourcing and responsi-

bilities for managing vendor and service-provider relationships?

3. Has the bank evaluated the adequacy of its insurance coverage to cover operational risks in its electronic banking activities?
4. Has the bank's legal counsel been involved in the development and review of electronic banking agreements (for example, agreements with third-party vendors)? Has the bank's legal counsel also been involved in the development and review of its authentication methods to ensure that the methods provide a foundation to enforce agreements and transactions and to validate the parties involved, consistent with applicable state laws?

Employee benefit trusts are specialized trusts most commonly established to provide retirement benefits to employees. However, they may also be established for employee stock ownership or thrift purposes, or to provide medical, accident, and disability benefits. There are qualified and unqualified plans. Retirement plans are qualified under section 401 of the Internal Revenue Code (IRC), and employee benefit trusts are tax exempt under section 501(a) of the IRC. The major types of qualified plans are profit sharing, money purchase, stock bonus, employee stock ownership plans (ESOPS), 401(k) plans, and defined benefit pension plans.

Since 1974, state jurisdiction of employee benefit trusts and their administration has been largely preempted by a comprehensive scheme of federal laws and regulations under the Employee Retirement Income Security Act of 1974 (ERISA). ERISA is divided into four titles: Title I, ''Protection of Employee Benefit Rights,'' includes the fiduciary responsibility provisions (in part 4) that are interpreted and enforced by the U.S. Department of Labor (DOL). Title II, ''Amendments to the Internal Revenue Code Relating to Retirement Plans,'' is similar to Title I, but the Internal Revenue Service (IRS) is responsible for its enforcement. Title III, ''Jurisdiction, Administration, Enforcement,'' grants jurisdiction and powers for administration to various governmental units. Title IV, ''Plan Termination Insurance,'' establishes the Pension Benefit Guaranty Corporation (PBGC). The PBGC ensures that defined benefit plans have sufficient resources to provide minimum levels of benefits to participants. In addition to the PBGC, the primary agencies that have promulgated necessary regulations and interpretations pursuant to ERISA are the DOL and IRS. However, state and federal banking agencies also have a recognized role under this statute.

Numerous laws affecting employee benefit plans have been enacted since the adoption of ERISA; however, the most sweeping changes were imposed by the Tax Reform Act of 1986. These changes include (1) imposing numerous excise taxes on employers and employees for failure to meet new plan contribution and distribution rules, (2) lowering the maximum amount of contributions and benefits allowed under qualified defined contribution and defined benefit plans, (3) lowering the amount an individual can contribute to a 401(k) plan, and (4) providing new nondiscrimination rules covering plan contributions and distributions. Virtually all qualified plans had to be amended to comply with this law.

A specific statutory provision of ERISA mandates the exchange of information among federal agencies. Accordingly, the federal banking agencies have entered into an agreement with the DOL whereby a banking agency noting any possible ERISA violations that meet certain specific criteria will refer the matter to the DOL.

ERISA imposes very complex requirements on banks acting as trustees or in other fiduciary capacities for employee benefit trusts. Severe penalties can result from violations of statutory obligations. With respect to a bank's own employees' retirement plan, the bank (or ''plan sponsor''), regardless of whether it is named trustee, is still a ''party-in-interest'' pursuant to the statute. Therefore, unless a transaction qualifies for narrowly defined statutory exemptions (or unless it is the subject of a specific ''individual'' exemption granted by the DOL), any transaction involving the purchase or sale of an asset of the plan from or to the bank, any affiliate, officer, or employee could constitute a prohibited transaction under ERISA.

The current and projected costs of employee benefit plans should be analyzed for their impact on the expenses and overall financial condition of the bank. Excessive pension or profit-sharing benefits, large expense accounts, employment contracts, or bonuses for officers or directors (especially if they are also large shareholders) could prove detrimental and even lead to civil liability for the bank or its board.

Depending on the type of plan and the allocations of its fiduciary duties, certain reporting, disclosure, and plan design requirements are imposed on the plan sponsor and/or its designated supervising committee. Therefore, a bank should have appropriate expertise, policies, and procedures to properly administer the type of employee benefit accounts established for its employees.

If an examiner, as part of any examination assignment, detects possible prohibited transactions, self-dealing, or other questionable activities involving the bank's employee benefit plan, an appropriate investigation should be undertaken. Substantial conversions of existing defined benefit plans or plan assets into holdings of bank or affiliate stock, under certain circumstances,

could involve ERISA violations. An examiner should refer a complicated question arising out of any of these situations to the examiner-in-charge for resolution or submission to the Reserve Bank.

Part I of the following examination procedures (section 4080.3) should be completed for every commercial bank examination; part II should also be completed if the employee benefit plan is not trusteed by the bank or by an affiliate bank subject to supervision by a federal banking agency. Parts I and II may be completed by a trust specialist, if available. When a bank trust department is named as trustee, the examiner should determine whether compliance with ERISA was reviewed during the previous trust examination. If not, then part II should be completed.

1. To determine if the policies, practices, procedures, internal controls, and available expertise regarding employee benefit trusts are adequate.
2. To determine if bank officers are operating in conformance with the established guidelines.
3. To evaluate the impact of employee benefit plans and related benefits on the financial condition of the bank.
4. To determine compliance with laws, regulations, and instrument provisions.
5. To initiate corrective action when policies, practices, procedures, or internal controls are deficient or when violations of laws, regulations, or the governing instruments have been noted.

PART I

1. If selected for implementation, complete or update the Employee Benefit Trusts section of the Internal Controls Questionnaire.
2. Test for compliance with policies, practices, procedures and internal controls in conjunction with performing the remaining examination procedures. Also obtain a listing of any deficiencies noted in the latest review done by internal/external auditors from the examiner assigned ''Internal Control,'' and determine if appropriate corrections have been made.
3. Determine the approximate number, size and types of employee benefit plans held for the benefit of the bank's officers and employees.
4. Obtain plan instruments or amendments thereto (if any) and summarize key features for the work papers. As appropriate, add or update the following information:
   a. Date of adoption of new plan or amendment and brief summary of the plan or amendment.
   b. Parties or committees named trustee and (if different) person(s) responsible for making investment decisions.
   c. Individuals, committees or outside parties named as responsible for plan administration.
   d. Basic investment/funding characteristics (e.g., ''non-contributory profit-sharing, up to 100% in own BHC stock;'' ''contributory defined benefit pension plan, purchasing diversified securities,'' etc.).
   e. Latest Form 5500 (IRS) filed for plan (may be omitted if plan administrator is an affiliate bank or bank holding company).

   Example: First Bank established a non-contributory profit sharing trust in 1975 for all officers and employees. Latest amendment, as of December 31, 19XX, made technical alterations to the vesting and forfeiture provisions. The most recent available valuation of the trust's assets, dated June 30, 19XX, indicated total assets of $22,093,000 (market value). Assets were comprised of U.S. government securities (42%), listed stocks (53%) and cash equivalents. Bank of _____, as trustee, has sole investment responsibility.
5. If a plan is a defined benefit pension plan, ascertain the actuarily-determined amount of unfunded pension liability, if any, and the bank's arrangements for amortization. (Note: Unfunded pension liability represents a contingent liability per instructions for the Report of Condition.)
6. Determine if the current and projected costs of the employee benefit plan(s) is reasonable in light of the bank's financial condition.

Complete part II of these procedures, if applicable, then continue to step 7, below. Part II is to be completed when a plan for the bank's employees is administered by the bank or a bank committee and is not trusteed by the bank itself or an affiliate bank subject to supervision by a federal banking agency.

7. Determine whether any instances of possible violations of ERISA have been noted, and that as to each such instance, full information has been developed for current workpapers to support a referral to DOL pursuant to SR-81-697/TR-81-46.

   Note: While the final decision on whether or not to make a referral to the DOL is to be made by the Board's staff after receipt of the report of examination, complete information should always be obtained regarding possible ERISA violations in the event the decision is made to refer the matter. If gathering certain of the information would impose an undue burden upon the resources of the examiners or the bank, Board's staff (Trust Activities Program) should be consulted. Where a significant prohibited transaction such as self dealing has taken place, the bank should be clearly informed that it is expected to undertake all such corrective and/or remedial actions as are necessary under the circumstances. One measure would be for the bank to apply to the DOL for a retroactive exemption under ERISA section 408(a).
8. Reach a conclusion concerning:
   a. The adequacy of policies, practices and

procedures relating to employee benefit trusts.
   b. The manner in which bank officers are operating in conformance with established policy.
   c. The accuracy and completeness of any schedules obtained.
   d. Internal control deficiencies or exceptions.
   e. The quality of departmental management.
   f. Other matters of significance.
9. Prepare in appropriate report format, and discuss with appropriate officer(s):
   a. Violations of laws and regulations.
   b. Recommended corrective action when policies, practices or procedures are deficient.
10. Update the workpapers with any information that will facilitate future examinations.

PART II

1. Review plan asset listings, valuations, or printouts obtained for any instances of possible prohibited transactions (ERISA sections 406(a) and (b)). The listings should include holdings of:
   a. Loans.
   b. Leases.
   c. Real Estate.
   d. Employer stock or other securities or obligations.
   e. Own bank time deposits.
   f. Other assets which might constitute, or result from, prohibited transactions.
2. Review transaction(s)/holding(s) in the previous step for conformity to:
   a. ERISA provisions regarding employer securities or real estate (sections 407(a), (b) and (c)) and related regulations.
   b. Statutory exemptions of ERISA (section 408(b)).
   c. ‘‘Exclusive benefit,’’ prudence and diversification requirements of ERISA (sections 404(a) and (b)).

Employee Benefit Trusts
Internal Control Questionnaire
Effective date December 1985

Section 4080.4

Review the bank's internal controls, policies, practices and procedures for employee benefit accounts. The bank's system should be documented in a complete and concise manner and should include, where appropriate, narrative descriptions, flowcharts, copies of forms used and other pertinent information. Part I should be completed as part of every examination; both parts I and II should be completed whenever the plan, administered by the bank or a bank committee, is *not* trusteed by the bank itself or by an affiliate bank subject to supervision by a federal banking agency.

PART I

1. Are new employee benefit plans, significant amendments thereto, and related costs and features approved by the bank's board of directors?

*2. Does the institution obtain and maintain on file the following minimum documentation:
   a. The plan and the corporate resolution adopting it?
   b. IRS ''determination'' or ''opinion'' letter substantiating the tax-exempt status of the plan?
   c. The trust agreement and the corporate resolution appointing the trustee(s), if applicable? (On occasion, fully insured plans may have no named trustee.)
   d. Amendments to the plan or trust documents?

3. If the bank or a committee of its officers and employees acts as plan administrator for any plan(s), does it have internal procedures and/or has it arranged by contract for external administrative expertise sufficient to assure compliance with reporting, disclosure and other administrative requirements of ERISA and related regulations?
4. Have the bank, its officers, directors or employees, or any affiliate(s) entered into any transactions to buy or sell assets to the bank's employee benefit plan(s)?
5. Do plan investments conform to instrument investment provisions?

PART II

1. When exercising fiduciary responsibility in the purchase or retention of employer securities or employer real estate, does the bank have procedures to assure conformity with ERISA section 407 and related provisions?

   Note: The requirements of ERISA and the associated DOL regulation with respect to ''employer securities and employer real estate'' include:
   a. A plan may not acquire or hold any but ''qualifying employer securities and employer real estate.''
   b. A defined benefit plan may hold no more than 10 percent of the fair market value of its assets in qualifying employer securities and/or qualifying employer real property, except as provided by ERISA sections 407(a)(3) or 414(c)(1) and (2), and adopted regulations.
   c. Any dispositions of such property from a plan to a party-in-interest shall conform to ERISA sections 414(c)(3) and (5) and adopted regulations, but certain acquisitions and sales may be made pursuant to the section 408(a) exemption.
   d. The plan instrument, for an eligible individual account plan which is to hold in excess of 10 percent of the fair market value of its assets in qualifying employer securities or real property, shall provide explicitly the extent to which such plan may hold such assets. [ERISA sections 407(b)(1) and (d)(3)]

2. Does the bank have procedures to ensure conformance to the following statutory exemptions (and associated regulations) from the prohibited transactions provisions of ERISA:
   a. Loans made by the plan to parties-in-interest who are participants or beneficiaries? [ERISA section 408(b)(1)]
   b. Investment in deposits which bear a reasonable rate of interest of a bank which is a fiduciary of the plan? [ERISA section 408(b)(4)]

   Note: Other statutory exemptions which may on occasion be applicable are:
   c. Arrangements for office space or legal, accounting or other necessary services? [ERISA section 408(b)(2)]
   d. Loans to employee stock ownership trusts? [ERISA section 408(b)(3)]

e. Transactions between a plan and a collective trust fund maintained by a party-in-interest which is a bank or trust company? [section 408(b)(8)]
f. Providing of any ancillary service by a bank or trust company which is a fiduciary of the plan? [ERISA section 408(b)(6)]

3. If exercising or sharing fiduciary responsibility, does the bank have procedures designed:
   a. To ensure that duties are executed for the exclusive benefit of plan participants and beneficiaries, in accordance with the ''prudent man'' standard? [ERISA sections 404(a)(1)(A) and (B)]
   b. To ensure that investments are diversified, unless it is clearly prudent not to do so or otherwise excepted by other provisions of ERISA? [ERISA section 404(a)(1)(C)]

INTRODUCTION

Market risk reflects the degree to which changes in interest rates, foreign exchange rates, commodity prices, or equity prices can adversely affect a financial institution's earnings or capital. For most community banks, market risk primarily reflects exposure to interest rate risk (IRR). While this risk is a normal part of banking and can be an important source of profitability and shareholder value, excessive levels of IRR can pose a significant threat to an institution's earnings and capital base. Accordingly, effective risk management that maintains IRR at prudent levels is essential to the safety and soundness of institutions.

The Interagency Guidelines Establishing Standards for Safety and Soundness (12 CFR 208, appendix D-1) require an institution to manage IRR in a manner that is appropriate to the size of the institution and the complexity of its assets and liabilities; and provide for periodic reporting to management and the board of directors regarding interest rate risk with adequate information for management and the board of directors to assess the level of risk. As a result, an important element of examinations and the supervisory process is the evaluation of an institution's exposure to changes in interest rates. Examiners evaluate both the adequacy of the management process used to control IRR and the quantitative level of exposure. In addition, examiners should assess the existing and potential future effects of changes in interest rates on an institution's financial condition, including the effect on the institution's capital adequacy, earnings, liquidity, and asset quality.

This section incorporates and builds upon the principles and guidance provided in four Supervision & Regulation (SR) letters:

- SR-93-69, "Examining Risk Management and Internal Controls for Trading Activities of Banking Organizations";
- SR-96-13, "Joint Policy Statement on Interest Rate Risk";[1]
- SR-10-1, "Interagency Advisory on Interest Rate Risk"; and
- SR-12-2, "Questions and Answers on Interagency Advisory on Interest Rate Risk Management."

1. See also 61 Fed. Reg. 33,166 (June 26, 1996).

TYPES AND SOURCES OF MARKET RISK

Market risk can arise from a variety of sources, including

- the overall structure of an institution's balance sheet, especially its loans, investments, and funding structure;
- its use of off-balance-sheet instruments (such as derivatives) for speculation; and
- its trading activities, if any.

While IRR is the most common form of market risk, market risk also arises from exposure to foreign exchange rates, commodity prices, and equity prices.

Foreign exchange risk surfaces when an institution, typically a larger or internationally active institution, performs foreign currency transactions on behalf of its customers, through either wire transfer activity or forward currency contracts. Institutions also may be exposed to currency fluctuations if they have a significant amount of investments denominated in foreign currencies. Institutions can be adversely affected when currencies in which they hold assets weaken or when currencies in which they have obligations strengthen. Foreign exchange risk also arises indirectly when changes in exchange rates affect the competitive position of an institution that operates in different countries.

Commodity price risk is similar to equity risk and encompasses the changes in an institution's earnings and asset values resulting from fluctuations in commodity prices. Some institutions are active in the commodity derivative market, offering derivative contracts linked to commodity prices. In addition, an institution's borrowers can be affected significantly by changes in commodity prices, such as the effect of fluctuating oil prices on airlines or in the realm of agricultural lending.

Equity price risk is the variation in profit or net worth caused by the changes in the prices of individual shares or the level of stock markets as a whole. Equity risk has both direct and indirect results. Fluctuations in stock prices will directly affect the value of shares, portfolios, and equity derivatives held by an institution. There also may be an indirect effect when declining equity prices affect the viability of a company to which

the bank has loaned money. Banks generally do not hold equity investments.

TYPES OF INTEREST RATE RISK

As previously discussed, IRR is the most common form of market risk for banking institutions. IRR can arise from a variety of sources, including repricing risk, yield curve risk, basis risk, options risk, and price risk. Various assets and liabilities may be exposed to more than one type of IRR.

Repricing risk is the primary and most discussed source of IRR and is the risk that the institution's assets, liabilities, and off-balance-sheet (OBS) instruments will reprice at different times or amounts. Repricing mismatches are fundamental to the business of banking and generally occur from either short term liabilities funding longer-term assets or long term liabilities funding shorter-term assets. Institutions whose liabilities reprice faster than their assets reprice are considered to be liability sensitive. The earnings of a liability sensitive institution generally increase when interest rates fall and decrease when rates rise. Conversely, an asset sensitive institution's assets reprice more quickly than their liabilities. These institutions' earnings generally benefit from a rising rate environment and are harmed by a falling rate environment.

Yield curve risk is the relationship between changing rates for the same instrument across a spectrum of maturities. It arises when assets and funding sources are linked to similar indexes with different maturities and the shape or slope of the yield curve changes by flattening, steepening, or inverting. For example, a 30-year Treasury bond's yield may change by 200 basis points; however, the three-year Treasury note's yield only changed by 50 basis points during the same time period.

Basis risk arises from a change in the relationship or spread between different market indexes. It occurs when the market indexes used to price assets and liabilities change by different amounts or at different times. For example, assume an operator uses a Treasury bill (T-bill) to hedge an interest rate risk in Eurodollars. The interest rates for T-bills and Eurodollars do not always move exactly parallel to each other. The risk of this lack of parallel movement is basis risk. The second occurs when the period of time for which a financial risk exists is not identical with the period of time for which the hedge is arranged, for example, when a three-month interest risk in a revolving Eurodollar loan is hedged with a six-month futures contract in Eurodollars. A change in the shape of the yield curve can bring about nonparallel movements in interest rates for the two different maturities.

Options risk is the risk arising from the options in assets, liabilities, and OBS instruments. An option provides the holder with the right, but not the obligation, to buy, sell, or, in some manner, alter the cash flow of an instrument or financial contract. Options may be distinct instruments, such as exchange-traded and over-the-counter contracts, or they may be embedded within the contractual terms of other instruments. Instruments with embedded options include bonds and notes with call or put provisions (e.g., callable U.S. agency notes), loans that give borrowers the right to prepay balances without penalty (e.g., residential mortgage loans), and various types of non-maturity deposit instruments that give depositors the right to withdraw funds at any time without penalty (e.g., demand deposits).

Price risk is the risk that the fair value of financial instruments will change when interest rates change. For example, trading portfolios, held-for-sale loan portfolios, and mortgage servicing assets contain price risk.

EFFECTS OF INTEREST RATE RISK

IRR can expose an institution's earnings and capital to adverse changes in market interest rates.

In assessing the effects of changing rates on earnings, institutions' measurement systems may focus on either net interest income or net income. In general, institutions focus primarily on net interest income—the difference between total interest income and total interest expense. However, interest rates can affect other income components, especially fee-based income. In particular, non-interest income generated by loan servicing and various asset-securitization programs can be highly sensitive to changes in market interest rates. Institutions with significant non-interest income that is sensitive to changing rates should have measurement systems in place that focus on net income.

Market interest rates also affect the value of an institution's assets, liabilities, and OBS instruments and, thus, effect the value of an institution's equity capital. The economic value of an instrument is an assessment of the present value of its expected net future cash flows, discounted to reflect market rates.[2] Interest rate changes can have a material effect on the economic value of an instrument. For example, the economic value of a bond with a fixed coupon rate generally falls in a rising rate environment. By evaluating changes in the institution's economic value for a given change in interest rates, institution management can identify risk arising from long-term repricing or maturity gaps as the interest rate environment may affect the institution's future earnings or capital values.

Historically, banks have managed their IRR exposures adequately and few have failed solely as a result of adverse interest rate movements. Changes in interest rates can have negative effects on profitability and need to be carefully managed, especially given the rapid pace of financial innovation and the heightened level of competition among all types of financial institutions.

ORGANIZATIONAL PROCESSES AND CONTROLS FOR MANAGEMENT OF INTEREST RATE RISK

Risk-Management Framework

As is the case in managing other types of risk, sound IRR management involves effective oversight and a comprehensive risk-management process that includes the following elements:

- effective policies and procedures designed to control the nature and amount of IRR, including clearly defined IRR limits and lines of responsibility and authority;
- appropriate risk-measurement, monitoring, and reporting systems; and
- effective internal controls that include an independent review and/or audit of key elements of the risk-management process.

The formality and sophistication used in managing IRR often varies by size and sophistication of the institution, the nature and complexity of its holdings and activities, and the overall level of its IRR. Less complex practices may be adequate for well-managed institutions with noncomplex activities and holdings that present a low IRR profile.

More complex institutions and those with higher IRR exposures or holdings of complicated instruments likely require sophisticated and formal IRR management systems to address their broader range of financial activities. In addition, formal IRR management systems generally will provide an institution's senior management with the needed information to monitor and direct day-to-day activities. The more complex IRR management processes often employed at these institutions may warrant a more thorough independent review and validation process of the IRR model utilized.

Individuals involved in the risk-management process should be sufficiently independent of business lines to ensure adequate separation of duties and avoid potential conflicts of interest. The degree of autonomy these individuals have may be a function of the size and complexity of the institution. In smaller institutions with limited resources, it may not be possible to completely remove individuals with business-line responsibilities from the risk-management process. In these situations, and assuming the institution engages in less complex activities, the institution's focus should be directed towards ensuring that risk-management functions are conducted appropriately. Larger, more complex institutions should have separate and independent risk-management units.

Board of Directors and Senior Management Oversight

The board of directors and senior management have unique yet complementary responsibilities related to the oversight and management of the institution's IRR risk profile.

2. For some instruments, the economic value of an instrument may be the same or differ from its fair value depending on the facts and circumstances. The fair value is an accounting term and is generally considered to be the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. For more information on fair value and the fair value measurement of derivatives, see ASC Topic 820, "Fair Value Measurement" as well as the Call Report instructions.

Board of Directors

The board of directors is ultimately responsible for establishing the institution's level of IRR. The board of directors or a board committee should oversee the establishment, approval, and periodic review of IRR management strategies, policies, procedures, and limits (or risk tolerances). In addition, the board or a board committee should understand the implications of the IRR strategies that the institution pursues, including their potential impact on market, liquidity, credit, and operational risks. To be appropriately informed about the institution's IRR exposure, the nature of risks in current and proposed new activities, and the adequacy of the institution's risk-management process, the board or its committee should receive reports from senior management that contain sufficient detail to assist in making informed policy decisions. The frequency of board reports depends on the complexity of the institution's holdings and the materiality of changes in its holdings.

Unlike senior management, the members of an institution's board of directors do not necessarily need to have detailed technical knowledge of complex financial instruments, legal issues, or sophisticated risk-management techniques. However, the institution's board of directors should oversee and hold senior management accountable for appropriately measuring, monitoring, and controlling IRR.

Senior Management

Senior management should be responsible for implementing

- adequate systems and standards for measuring risk,
- standards for valuing positions and measuring performance,
- a comprehensive IRR reporting and monitoring process, and
- effective internal controls and review processes.

Senior management should be responsible for implementing board-approved strategies, policies, and procedures as well as managing IRR within the designated lines of authority and responsibility. Senior management should develop and implement policies and procedures that align with the board's goals, objectives, and risk limits. Senior management should be responsible for overseeing institution personnel to confirm that operating standards are being followed. Further, senior management should assure that institution personnel who perform analysis and risk-management activities related to IRR have the technical knowledge, depth, and experience commensurate with the nature and scope of the institution's activities.

Reports to senior management should provide aggregate information as well as sufficient supporting detail, so that management can assess the sensitivity of the institution to changes in market conditions and other important risk factors. Effective IRR reports generally include measurement of IRR exposures relative to limits and disclosure of key assumptions. Senior management should also periodically review the institution's IRR management policies and procedures to assess the appropriateness of its risk management. Senior management should also discuss risk-measurement, reporting, and management procedures with risk-management staff. These discussions will assist senior management in developing and providing IRR reports to the board of directors that contain sufficient detail to assist in making informed policy decisions for the institution.

Policies, Procedures, and Limits

Institutions should have clear policies and procedures for limiting and controlling IRR. In general, these policies and procedures should

- delineate lines of responsibility and accountability over IRR management decisions,
- clearly define authorized instruments and permissible hedging and position-taking strategies,
- identify the frequency and method for measuring and monitoring IRR, and
- specify quantitative limits that define the acceptable level of risk for the institution.

In addition, management should define the specific procedures and approvals necessary for exceptions to policies, limits, and authorizations. All IRR risk policies should be reviewed by management and approved by the board of directors at least annually and revised as needed.

Clear Lines of Authority

Whether through formal written policies or operating procedures, management should define the structure of managerial responsibilities, oversight, and lines of authority in the following areas:

- developing and implementing strategies and tactics used in managing IRR
- establishing and maintaining an IRR measurement and monitoring system that is commensurate with the institution's size and complexity
- identifying potential IRR and related issues arising from the use of new products
- developing IRR management policies, procedures and limits, and authorizing exceptions to policies and limits

Individuals and management committees responsible for making decisions about IRR management should be clearly identified. Most institutions delegate IRR management responsibilities to a committee of senior managers, sometimes called an asset/liability committee (ALCO). At these institutions, policies identify the ALCO membership, the committee's duties and responsibilities, the extent of its decisionmaking authority, and the form and frequency of its reports to senior management and the board of directors. An ALCO should have sufficiently broad participation across major banking functions (for example, lending, investment, deposits, and funding) so that its decisions can be executed effectively throughout the institution. In many large institutions, the ALCO delegates day-to-day responsibilities for IRR management to an independent risk-management department or function.

Individuals involved in the IRR management process (including separate risk-management units, if present) should be sufficiently independent from the business lines, including through the reporting structure, to provide for adequate separation of duties and avoid potential conflicts of interest. Also, personnel charged with measuring and monitoring IRR should have a well-founded understanding of the institution's IRR profile. Compensation policies for these individuals should be adequate enough to attract and retain personnel who are well qualified to assess the risks of the institution's activities, and are compatible with effective controls and risk management.

Authorized Activities

Institutions should clearly identify the types of financial instruments that are permissible for managing IRR, either specifically or by their characteristics. As appropriate to its size and complexity, the institution should delineate procedures for acquiring specific instruments, managing individual portfolios, and controlling the institution's aggregate IRR exposure. Major hedging or risk-management initiatives should be approved by the board or board committee before being implemented.

Before introducing new products, hedging, or position-taking initiatives, management should also determine whether there are adequate operational procedures and risk-control systems in place and whether procedures need to be revised.

Risk Limits

The goal of IRR management is to maintain an institution's IRR exposure within self-imposed parameters over a range of possible changes in interest rates. A system of IRR limits and risk-taking guidelines assists an institution in achieving that goal. Such a system should set limits for the institution's level of IRR and, where appropriate, provide the capability to allocate these limits to individual portfolios or activities. Systems should also identify for management when a limit is violated to allow for prompt management attention. Further, in the event of a limit violation, an institution's processes should address specific escalation procedures outlining designated responsible personnel and risk mitigation procedures.

Risk limits should be appropriate to the size, complexity, and financial condition of the institution. Depending on the nature of an institution's holdings and general sophistication, limits can be identified for individual business units, portfolios, instrument types, or specific instruments.[3] The level of detail of risk limits should reflect the characteristics of the institution's holdings, including the various sources of IRR to which the institution is exposed. Limits applied to portfolio categories and individual instruments should be consistent with and complementary to consolidated limits. For exam-

3. This manual's section on "Investment Securities and End-User Activities" discusses issues in setting price volatility limits in the acquisition of securities and derivatives.

ple, an institution should consider whether

- IRR limits are consistent with the institution's overall approach to measuring and managing IRR and address the potential impact of changes in market interest rates on both reported earnings and the institution's economic value of equity (EVE);
- limits are consistent with the risk tolerance of the board of directors;
- IRR tolerances address the potential impact of changing interest rates on capital and earnings from a short-term and a long-term perspective;
- limits on the IRR exposure of earnings, which primarily address short term exposure, are broadly consistent with those used to control the exposure of an institution's economic value, which reflects long term exposure;
- IRR limits and risk tolerances consider specific scenarios of market interest rate movements, such as an increase or decrease of a particular magnitude; and
- the rate movements used in developing these limits represent meaningful stress situations, taking into account historic rate volatility and the time required for management to address exposures.

Interest Rate Risk Monitoring and Reporting

An effective process of measuring, monitoring, and reporting exposures is essential for adequately managing IRR. The sophistication and complexity of this process should be appropriate to the size, complexity, nature, and mix of an institution's business lines and its IRR characteristics.

Effective IRR measurement systems monitor the effect of rate changes on both earnings and economic value. The latter is particularly important for institutions with significant holdings of intermediate and long-term instruments or instruments with embedded options because their market values can be particularly sensitive to changes in market interest rates.

IRR measurement systems should

- assess material IRR associated with an institution's assets, liabilities, and OBS positions;
- use generally accepted financial concepts and risk-measurement techniques; and
- have well-supported assumptions and parameters.

In many cases, the interest rate characteristics of an institution's largest holdings will dominate its aggregate risk profile. While all of an institution's holdings should receive appropriate treatment, measurement systems should provide more detailed information on the major holdings and instruments whose values are especially sensitive to rate changes. The IRR measurement system should have sufficient functionality and sophistication to properly identify and value instruments with significant embedded or explicit option characteristics.

An accurate, informative, and timely management information system is essential for managing IRR exposure, and ensuring risks and activities align with the institution's policies and risk tolerance. Reporting of risk measures should be regular and clearly compare current exposure with the institution's internal risk limits. In general, senior management should receive quarterly reports on the institution's IRR profile. The reports should utilize current and accurate data. More frequent reporting may be appropriate depending on the institution's exposure to IRR and the potential for significant changes to the institution's capital and earnings. In addition, past forecasts or risk estimates should be compared with actual results as one tool to identify any potential shortcomings in modeling techniques.[4]

The types of reports prepared for the board and for various levels of management will vary based on the institution's IRR profile. Effective IRR reports enable senior management to

- evaluate the level of and trends in the institution's aggregate IRR exposure;
- demonstrate and verify compliance with the institution's policies and limits;
- evaluate the sensitivity and reasonableness of key assumptions;
- assess the results and future implications of major hedging or position-taking initiatives that have been taken or are being actively considered;
- understand the implications of various stress scenarios, including those involving breakdowns of key assumptions and parameters;
- review IRR policies, procedures, and the

4. For more information, see SR-11-7, "Guidance on Model Risk Management."

adequacy of the IRR measurement systems; and
- determine whether the institution holds sufficient capital for the level of risk being taken.

IRR Measurement Methods

There are a number of techniques to measure the IRR exposure of both earnings and economic value. Their complexity ranges from simple calculations and static simulations using current holdings to highly sophisticated dynamic modeling techniques that reflect potential future business and business decisions. Regardless of the methods used, an institution's IRR measurement system should be sufficiently robust to capture material on and off-balance-sheet positions and incorporate a stress-testing process to identify and quantify the institution's IRR exposure and potential problem areas.

The most common types of IRR measurement systems are

- Gap Analysis
- Earnings Simulation Analysis
- Economic Value of Equity (EVE)

Each risk-measurement system has limitations and vary in the degree of its ability to capture various components of IRR. The following exhibit demonstrates the types of interest rate exposures that each measurement system generally addresses. While different methodologies capture different risk exposures, outputs from all models should generally provide a consistent view of IRR trends. If divergent outcomes occur, they are typically due to the structure of the balance sheet, the interest rate environment, the timing of asset/liability mismatches, the sensitivity of funding sources to interest rate changes, or the volume of fixed or floating rate assets. Institution management should understand the nature and underlying reasons for material differences in outputs.

Gap analysis is a basic IRR measurement technique utilizing a maturity/repricing schedule, which distributes assets, liabilities, and OBS holdings into time bands according to their final maturity (if fixed rate) or time remaining to their next repricing (if floating). The choice of time bands may vary from institution to institution. Those assets and liabilities lacking contractual repricing intervals or maturities are assigned to repricing time bands according to the judgment and analysis of the institution.

Table 1—Interest Rate Exposures by Measurement Systems

	Gap Analysis	Earnings Simulation Analysis	Economic Value of Equity
Short-term earnings exposure	Yes	Yes	Limited*
Long-term exposure	Yes	Limited*	Yes
Repricing risk	Yes	Yes	Yes
Yield curve risk	Limited*	Yes	Yes
Basis risk	Limited*	Yes	Limited*
Option risk	Limited*	Limited*	Yes
Price risk	Limited*	Limited*	Yes

*Depending on the sophistication of the model and the manner in which it is used

Gap analysis can be used to generate rough indicators of the IRR sensitivity of both earnings and economic values to changing interest rates. To evaluate earnings exposures, liabilities arrayed in each time band can be subtracted from the assets arrayed in the same time band to yield a dollar amount of maturity/repricing mismatch or gap in each time band. The direction and magnitude of the gaps in various time bands can demonstrate potential earnings volatility arising from changes in market interest rates. A maturity/repricing schedule also can evaluate the effects of changing rates on an institution's economic value.

Typically, gap analysis includes ratios of rate-sensitive assets to rate-sensitive liabilities in given time periods. Within a given time band, an institution may have a positive, negative, or neutral gap. An institution with a positive gap is "asset sensitive" for the given time band because more assets than liabilities are subject to repricing. An institution with a negative gap is "liability sensitive" for the given time band because more liabilities than assets are subject to repricing. An institution with a neutral gap (a ratio of rate-sensitive assets to rate-sensitive liabilities equal to one) is neither asset nor liability sensitive for the given time band.

At the most basic level, mismatches or gaps in

long-dated time bands can provide insights into the potential vulnerability of the economic value of relatively noncomplex institutions. However, gap analysis alone is generally not suitable for adequately assessing the institution's risk profile for the large majority of institutions. Long-term gap calculations, along with simple maturity distributions of holdings, may be sufficient for relatively noncomplex institutions with basic balance sheets, minimal optionality, and mainly repricing risk.

Earnings simulation analysis estimates cash flows and resulting earnings streams over a specific time period under various interest rate scenarios to estimate the effect of interest rate changes on net interest income or net income. For assessing the exposure of earnings, simulations estimating cash flows and resulting earnings streams over a specific period are conducted based on existing holdings and assumed interest rate scenarios. A simulation model's accuracy depends on the use of accurate assumptions and data.

A key aspect of IRR simulation involves the selection of an appropriate time horizon(s) over which to assess IRR exposures. Simulations can be performed over any time horizon and often are used to analyze multiple horizons identifying short-term, intermediate-term, and long-term risk. Utilizing a two-year time period generally is effective when using earnings simulation models. A two-year time frame effectively captures an institution's important transactions, tactics, and strategies to increase revenues, which can be hidden by viewing projected results within shorter time horizons. However, to assess the effects of certain products with embedded options, IRR simulations over longer time horizons (five-to-seven years) are typically needed.

Income simulations are static or dynamic. Static simulations are based on current holdings and assume a constant balance sheet with no new growth. Dynamic simulations include assumptions of asset growth, changes in existing business lines, new business, or changes in management or customer behaviors. Dynamic earnings simulation models can be useful for business planning and budgeting purposes. However, dynamic simulations are highly dependent on key variables and assumptions and can be inaccurate over an extended period. Furthermore, model assumptions, such as growth, can potentially hide underlying risk exposures. Therefore, static and dynamic simulations, in tandem, should be used to provide a more complete description of the institution's IRR exposure.

Economic value of equity (EVE) models consider the present value of expected cash flow over the entire expected life of the institution's holdings. EVE models simulate various interest rate scenarios to estimate the changes in an institution's economic value of capital as a result of changes in interest rates. This approach focuses on a longer-term time horizon, captures future cash flows expected from existing assets and liabilities, and is effective in considering embedded options in a typical institution's portfolio.

Most EVE models use a static approach by providing a snapshot in time of the risk inherent in the portfolio or balance sheet. However, some institutions incorporate dynamic modeling techniques that provide forward-looking estimates of economic value.

When utilizing EVE methods, institution management should establish appropriate EVE risk limits. Appropriate limits generally are based on the change of economic capital rather than absolute levels of economic capital. The accuracy of the assumptions in the model are critically important in the EVE model's ability to calculate the future cash flows of the institution's instruments. Unreasonable assumptions can lead to pronounced output errors in EVE models. As such, institution management should understand the significance and accuracy of assumptions by conducting sensitivity testing.

IRR Scenarios

IRR exposure estimates, whether linked to earnings or economic value, use some form of forecasts or scenarios of possible changes in market interest rates. Institution management should measure IRR exposure estimates over a probable range of potential interest rate scenarios, including meaningful stress situations. The scenarios should adequately cover the institution's meaningful sources of IRR associated with its holdings. In developing appropriate scenarios, institution management should consider the current level and term structure of rates and possible changes to that environment, given the historical and expected future volatility of market rates.

There are various common rate scenarios, including rate shock, rate ramp, stair step, and

non-parallel yield curve shifts. A rate-shock scenario is the most commonly used. In this scenario, rate changes are instantaneous and sustained. For instance, a plus 300 basis-point, rate-shock scenario would consist of the full 300 basis-point interest rate increase occurring in the first period measured and remain in effect for all measured periods. A rate ramp scenario consists of rate changes applied gradually over a measured period, such as a 300 basis-point rate increase during a 12-month period with rates rising 25 basis points each month. A stair-step scenario also consists of rate changes applied gradually; however, the changes are administered at less frequent intervals. For example, a 300 basis-point increase might be measured over a two-year period with rates increasing 50 basis points per quarter the first year and 25 basis points per quarter the second year. Nonparallel yield curve shifts are scenarios in which the yields do not change by the same number of basis points for every maturity, such as flattening, steepening, or inversion of the yield curve.

Effective scenarios conducted by institution management typically include an instantaneous plus or minus 200 basis-point parallel shift in market rates (rate shock). However, those scenarios alone may not adequately assess an institution's IRR exposure. As such, institutions should also consider utilizing changes in rates of greater magnitude, such as plus or minus 300 and 400 basis-point shocks. More sophisticated analyses involve the use of multiple scenarios, including the potential effects of changes in the relationships among interest rates (option risk and basis risk) and changes in the general level of interest rates and changes in the shape of the yield curve.

Data Integrity

In addition to validity of the underlying assumptions, and IRR scenarios used to model IRR exposures, the usefulness of IRR measurements depends on the integrity of the data on current holdings. Simulation techniques that rely heavily on specific assumptions should be used carefully because they rely on specific assumptions and parameters, which can lead to inaccurate reports if the underlying data is inaccurate.

The integrity of data on current positions is an important component of the risk-measurement process. Management should ensure that all material positions are represented in IRR measures, and that the data used are accurate and meaningful. IRR measurement techniques should reflect relevant repricing and maturity characteristics on key holdings. When applicable, data should include information on the contractual coupon rates and cash flows of associated instruments and contracts. Manual adjustments to underlying data should be supported and controlled.

Account Aggregation

Account aggregation is the process of grouping and measuring accounts of similar types and cash flow characteristics. The account aggregation process should be supported and periodically reviewed. The level of account aggregation from transaction systems into the IRR model will vary from one institution to another based the complexity of the accounts and the sophistication of the IRR model. Institutions should appropriately aggregate current account positions by meaningful characteristics (for example, by instrument type, coupon rate, or repricing characteristic). This allows the institution to appropriately measure material types and sources of IRR, including those arising from explicit or embedded options. Both contractual and behavioral characteristics should be considered when determining the cash flow patterns of accounts to aggregate.

Assumptions

Assumptions should be documented and their effects should be well understood by management. Management should review the assumptions used in assessing the interest rate sensitivity of complex instruments, such as those with embedded options, and instruments with uncertain maturities. Management should assess the consistent replacement growth rate assumptions if the ban uses dynamic simulations of future growth and business assumptions. Assumptions about customer behavior and new business should consider historical patterns and be consistent with the interest rate scenarios used. Institutions should review the reasonableness of assumptions covering asset prepayments, nonmaturity deposit price sensitivity and decay rates, and key rate drivers for each interest rate

shock scenario.[5]

The following discussion provides background information on the types of assumptions used in IRR models.

Driver rates and betas. Driver rates are utilized in most earnings simulations and economic value models and represent the rate or rates which drive the re-pricing characteristics of assets and liabilities. Examples of driver rates include the fed funds rate, U.S. Treasury yields, and the Wall Street Journal Prime rate. Depending on the sophistication of the model, a variety of driver rates may be tailored to the different products the institution offers. While institution rates generally move in relation to a driver rate, the movement may be less or more than the movement in the driver rate depending on management's pricing strategies. Most models utilize a beta factor to serve as a proxy for management's reaction to market changes. A beta factor represents the magnitude of the changes in the rates of bank products compared to the changes in the driver rates. For example, management may be expected to only increase deposit rates by 40 basis points for every 100 basis points move in the fed funds rate, resulting in a beta factor of 40 percent. Beta factors should be based on an analysis of the relationship between the product and the driver rate. To help determine the beta, management can perform correlation or regression analysis to quantify the historical relationship between the product and the drivers.

Non-maturity deposits. Assumptions about non-maturity deposits are critical as non-maturity deposits represent a large portion of the industry's funding base. An institution's IRR measurement system should consider the sensitivity of non-maturity deposits, including demand deposits, negotiable order of withdrawal accounts, savings deposits, and money market deposit accounts. There are a variety of techniques used to analyze IRR characteristics, and each institution should use a technique that is commensurate to the size, sophistication, and complexity of the institution. In general, treatment of non-maturity deposits should consider the historical behavior of the institution's deposits; general conditions in the institution's markets, including the degree of competition it faces or likely to face; and anticipated pricing behavior under the scenario investigated.

As non-maturity deposits have no contractual maturity date, institutions should utilize assumptions that determine the maturity of the accounts. The most common assumption utilized is a decay rate. Also, institutions experiencing or projecting capital levels that trigger brokered and high interest rate deposit restrictions should adjust deposit assumptions accordingly.[6]

Assumptions, including deposit betas and decay rates, should be supported to the fullest extent practicable. Treatment of non-maturity deposits within the measurement system may, of course, change from time-to-time based on market and economic conditions. Such changes should be well founded and documented. Treatments used in constructing earnings simulation assessments should be conceptually and empirically consistent with those used in developing EVE assessments of IRR.

Asset prepayment. Prepayment assumptions reflect the optionality and prepayment risk associated with loans and mortgage-related securities and are critical as cash flows may be received more quickly or more slowly than anticipated. Prepayments are highly influenced by the direction of interest rates as loan prepayments generally slow during periods of rising rates. Prepayment assumptions should take into consideration various factors, such as aging, geographic location, loan size, and fixed versus variable rates.

Stress Testing

Stress testing, which includes both scenario and sensitivity analysis, is an important part of IRR management. An institution's risk-measurement system for IRR should contain a meaningful evaluation of the effect of stressful market conditions on the institution. Stress scenarios should be designed to provide information on the kinds of conditions under which the institution's strategies or positions would be most vulnerable; thus, testing may be tailored to

5. A decay rate estimates the amount of existing non-maturity deposit that will run off over a given time period. Generally, rate-sensitive and higher-cost deposits, such as brokered and Internet deposits, should reflect higher decay rates than other types of deposits.

6. Section 38 of the FDI Act (12 U.S.C. 1831o) requires insured depository institutions that are undercapitalized to receive approval before engaging in certain activities, and further restricts interest rates paid on deposits by institutions that are not well capitalized. Section 38 restricts or prohibits certain activities and requires an insured depository institution to submit a capital restoration plan when it becomes undercapitalized.

the risk characteristics of the institution. Possible stress scenarios might include more severe changes in the term structure of interest rates, substantial rate changes over time, relationships among key market rates (basis risk), or volatility of market rates. The stress testing of assumptions used for illiquid instruments and instruments with uncertain contractual maturities, such as core deposits, is particularly critical to achieving an understanding of the institution's risk profile. Therefore, stress scenarios may include extremes of observed market conditions and plausible worst-case scenarios.

Management should conduct sensitivity analysis of the assumptions having the largest influence on an institution's model output under stressful situations. This sensitivity analysis may consist of testing key assumptions or variables by changing the variable in question while keeping all other variables constant and comparing the results to the base-case scenario. Based on the results of sensitivity analysis, management should be able to identify the assumptions which have the most impact on model output. This enables management to focus their efforts in verifying the most salient assumptions. Additionally, sensitivity analysis can be used to determine the conditions under which key business assumptions and model parameters or when IRR may be exacerbated by other risks or earnings pressures.

Internal Controls

An important element of an institution's internal controls for IRR is senior management's comprehensive evaluation and review of the various components of the IRR management process. Although procedures for establishing limits and adhering to them may vary among institutions, periodic control reviews should be conducted to determine whether the organization enforces its IRR policies and procedures. Senior management should promptly address situations where interest rate positions exceed established internal risk limits. Issues should be resolved based on processes described in approved policies. The institution should conduct periodic reviews of IRR management process. Reviews should also be conducted in light of significant changes since the last review, such as the nature of instruments acquired, as well as modifications to risk-measurement methodologies, limits, and internal controls.

Validating IRR models is a fundamental part of any institution's system of internal controls. An important element of model validation is independent review of the model's logical and conceptual soundness. The scope of the independent review should assess the institution's measurement of IRR, including the reasonableness of assumptions, the process used in determining assumptions, and the back testing of assumptions and results. Management also should implement adequate follow-up procedures to monitor the institution's corrective actions. The results of these reviews should be available for the relevant supervisory authorities.

Smaller institutions that do not have the resources to staff an independent review function should have processes in place to ensure the integrity of the various elements of their IRR management processes. Often, smaller institutions will use an internal party that is sufficiently removed from the primary IRR functions or an external auditor to independently verify the integrity of the IRR models used. More robust model validations processes for measurement systems are appropriate for institutions with complex risk exposures. These processes should include review by external auditors or other knowledgeable outside parties to ensure the IRR models' adequacy and integrity. Since measurement systems may incorporate one or more subsidiary systems or processes, institutions should ensure that multiple component systems are well integrated and consistent in all critical respects.

The frequency and extent to which an institution should reevaluate its risk-measurement methodologies and models depends, in part, on the specific IRR exposures created by their holdings and activities, the pace and nature of changes in market interest rates, and the extent to which there are new developments in measuring and managing IRR. In general, an institution should review its underlying IRR measurement methodologies and IRR management process annually, and more frequently as institution behaviors and market conditions dictate.

SUPERVISORY CONSIDERATIONS IN ASSESSING IRR SENSITIVITY TO MARKET RISK

Quantitative Level of IRR Exposure and Effect on Earnings and Capital

Examiners evaluating the quantitative level of IRR should review and assess the effects of past and potential changes in interest rates on an institution's financial condition, particularly its earnings, capital, liquidity, and, in some cases, asset quality. This assessment involves a broad analysis of an institution's business mix, balance-sheet composition, OBS holdings, and holdings of interest rate-sensitive instruments. Examiners should understand the institution's material holdings, and assess how changes in interest rates might affect the institution's financial performance. While the scope of the assessment should reflect the size, sophistication, and nature of the institution's holdings, primary areas of review include

- major on- and off-balance-sheet positions,
- concentrations in interest-sensitive instruments,
- the existence of highly volatile instruments, and
- significant sources of noninterest income that may be sensitive to changes in interest rates.

IRR Exposure to Earnings and Capital

An institution's IRR exposure should be assessed in terms of the potential effects on the institution's earnings and capital. When evaluating the potential effects of changing rates on an institution's earnings, examiners will assess the key determinants of the net interest margin, the effect that fluctuations in net interest margins can have on overall net income, and the rate sensitivity of non-interest income and expense. Analyzing the historical behavior of the net interest margin, including the yields on major assets, liabilities, and off-balance-sheet positions that make up that margin, can provide useful insights into the relative stability of an institution's earnings. Examiners should evaluate the exposure of earnings to changes in interest rates relative to the institution's overall level of earnings and the potential length of time such exposure might persist.

Exposures that would result in a significant decline in net interest margins or net income should prompt further investigation of the adequacy and stability of earnings and the adequacy of the institution's risk-management process. Specifically, in institutions exhibiting significant earnings exposures, examiners should emphasize the results of the institution's stress tests to determine the extent to which more significant and stressful rate moves might magnify the erosion in earnings identified in the more modest rate scenario.

When determining the amount of IRR exposure in context of capital, examiners will consider the effect of changes in market interest rates on the economic value of equity, level of embedded losses in the bank's financial structure, and impact of potential rate changes on the institution's earnings.

Examiners should take into account the absolute level of an institution's earnings or capital both before and after the estimated IRR shock. Institutions with strong earnings and capital can withstand greater shocks, whereas institutions with already less than satisfactory earnings or capital may warrant greater supervisory concern at relatively small IRR shocks.

Qualitative Assessment of Interest Rate Risk Management

When evaluating interest rate risk management at an institution, examiners should place primary consideration on the following elements of a sound risk-management system:

- board of directors and senior management oversight;
- policies, procedures, and limits;
- risk monitoring and management information systems; and
- internal controls.[7]

Through discussions with appropriate institution personnel, examiners should determine whether the institution has established appropriate corporate governance processes (internal

7. These elements are consistent with the guidance provided in SR-16-11, "Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $50 Billion."

policies, procedures, risk limits, and strategies), and whether the board of directors, or a committee thereof, is regularly informed about the level and trend of IRR, and reviews conformance with internal IRR policy limits and risk tolerances. If inadequacies are noted, examiners should communicate these findings to the institution and discuss strategies to improve the institution's corporate governance processes.

Examiners should determine whether internal measurement processes and systems are adequate. In particular, examiners should review the institution's input process by focusing on the procedures for entering and reconciling system data, categorizing and aggregating account data, ensuring the completeness of account data, and assessing the effectiveness of internal controls. In addition, examiners should review the results of the audit or independent reviews, and determine whether the results were appropriately reported to the board of directors, or a committee thereof, and whether the results revealed significant deficiencies.

EXAMINATION PROCESS

Examiners should assess and assign a rating to the sensitivity to market risk component, or "S" component, of the CAMELS rating system, at each full-scope examination.[8] To meet examination objectives efficiently and effectively while remaining sensitive to potential burdens imposed on institutions, the examination of sensitivity to market risk should follow a structured, risk-focused approach. A fundamental tenet of this approach is that supervisory resources are targeted at functions, activities, and holdings that pose the most risk to the safety and soundness of an institution. Accordingly, institutions with low levels of IRR would be expected to receive relatively less supervisory attention than those with more severe IRR exposures.

Many institutions have become especially skilled in managing and limiting the exposure of their earnings to changes in interest rates. Accordingly, for most banks and especially for smaller institutions with less complex holdings, the IRR element of the examination may be relatively simple and straightforward. On the other hand, some banks consider IRR an intended consequence of their business strategies and choose to take and manage that risk explicitly—often with complex financial instruments. These banks, along with banks that have a wide array of activities or complex holdings, generally should receive greater supervisory attention.

Examination Scope and Off-Site Analysis

During the examination scoping process prior to the on-site examination, examiners should use surveillance metrics and supervisory judgment, to determine bank's risk tier (low, moderate, or high). The scope of the examination work program should align with the bank's risk classification. More information on the use of surveillance metrics during the examination scoping process is discussed in this manual's section entitled, "Community Bank Supervision Process."

Additionally, examiners should assess the level of IRR exposure and the quality of IRR management to the fullest extent possible during the scoping process by reviewing the following:

- organizational charts and policies identifying authorities and responsibilities for managing IRR;
- IRR policies, procedures, and limits;
- ALCO committee minutes and reports (from 6 to 12 months before the scope visit);
- board of director reports on IRR exposures;
- audit reports (both internal and external);
- most recent IRR report, including assumptions used in the model; and
- Federal Reserve surveillance reports and supervisory screens.

If the examiners' assessment of the risk tier differs from the initial quantitative risk tier, examiners should adjust the risk tier. Adjustments to the risk tier during the scoping process based on examiner judgement should be rationalized and documented in the appropriate work papers.

During the Examination

Examiners should complete the appropriate examination procedures based on the bank's assigned risk tier. During the examination, the

8. There may be instances where the assessment of sensitivity to market risk is a topic of a targeted examination.

examiner-in-charger and the examiner working the IRR portion of the examination should confirm the risk classifications on which planned work programs were based and, if needed, adjust or expand the work programs. If initial discussions with management or additional information obtained during the examination indicates significant weakness in the bank's risk management or higher-than-anticipated risk, examiners should modify the examination's scope and work programs accordingly. All examination work programs are to include the review and verification of corrective action taken to address any outstanding Matters Requiring Immediate Attention (MRIAs) or Matters Requiring Attention (MRAs).

Material weakness in risk management or high levels of IRR exposure relative to earnings and capital may require corrective action. If an examiner determines that an IRR weakness warrants corrective action based on safety and soundness, the examiner, in consultation with the examiner-in-charge, should outline any MRIAs or MRAs.

When issuing a supervisory finding (including through the issuance of an MRIA or MRA), examiners will not criticize an institution for a "violation" of supervisory guidance (as supervisory guidance is not legally binding). When appropriate, examiners may reference (including in writing) supervisory guidance (such as interagency statements, advisories, bulletins, and policy statements) to provide examples of safe-and-sound conduct, appropriate risk-management practices, and other approaches to addressing compliance with laws or regulations.[9]

Assessing CAMELS Ratings

For most banks, IRR is the primary market risk exposure. Accordingly, the CAMELS market-risk sensitivity or "S" rating for most banks should be based on assessments of the adequacy of IRR management practices and the quantitative level of IRR exposure.[10] In particular, the "S" rating for most banks where IRR is the primary market risk exposure should be based on an assessment of the following evaluation factors:

- the sensitivity of the bank's earnings or the economic value of its capital to adverse changes in interest rates;
- the ability of management to identify, measure, monitor, and control exposure to interest rate risk given the bank's size, complexity, and risk profile;
- the nature and complexity of interest rate risk exposure arising from non-trading positions; and
- where appropriate, the nature and complexity of market-risk exposure arising from trading and foreign operations.

In addition to these listed factors, there may be additional factors that may be appropriate for the examiner to evaluate as part of determining the "S" rating for a bank.

The "S" component rating definitions of the CAMELS rating system are as follows:

1. A rating of "1" indicates that interest rate risk sensitivity is well controlled and that there is minimal potential that the earnings performance or capital position will be adversely affected. Risk-management practices are strong for the size, sophistication, and market risk accepted by the institution. The level of earnings and capital provide substantial support for the degree of interest rate risk taken by the institution.
2. A rating of "2" indicates that interest rate risk sensitivity is adequately controlled and that there is only moderate potential that the earnings performance or capital position will be adversely affected. Risk-management practices are satisfactory for the size, sophistication, and interest rate risk accepted by the institution. The level of earnings and capital provide adequate support for the degree of interest rate risk taken by the institution.
3. A rating of "3" indicates that control of interest rate risk sensitivity needs improvement or that there is significant potential that the earnings performance or capital position will be adversely affected. Risk-management practices need to be improved given the size, sophistication, and level of risk accepted by the institution. The level of earnings and capital may not adequately support the degree of interest rate risk taken by the institution.

9. SR-18-5/CA-18-7, "Interagency Statement Clarifying the Role of Supervisory Guidance."

10. "Overall Conclusions Regarding Condition of the Bank: Uniform Financial Institutions Rating System," provides guidance on the market-risk sensitivity component of the CAMELS rating system.

4. A rating of "4" indicates that control of interest rate risk sensitivity is unacceptable or that there is high potential that the earnings performance or capital position will be adversely affected. Risk-management practices are deficient for the size, sophistication, and level of risk accepted by the institution. The level of earnings and capital provide inadequate support for the degree of interest rate risk taken by the institution.
5. A rating of "5" indicates that control of interest rate risk sensitivity is unacceptable or that the level of risk taken by the institution is an imminent threat to its viability. Risk-management practices are wholly inadequate for the size, sophistication, and level of interest rate risk accepted by the institution.

The adequacy of a bank's IRR management is a leading indicator of its potential IRR exposure. Therefore, assessment of IRR management practices should be the basis for the overall assessment of a bank's IRR. Unsafe exposures and management weaknesses should be fully reflected in "S" ratings. Unsafe exposures and unsound management practices that are not resolved during the on-site examination should be addressed through subsequent follow-up actions by the examiner and other supervisory personnel.

1. Do the bank's assets, investments, deposits, other funding sources, and financial derivatives present a low or well-controlled level of interest rate risk?
2. Have adequate corporate governance processes (policies, procedures, risk limits, and strategies) been established?
3. Are internal measurement processes and systems adequate?
4. Are model inputs and management's assumption development process adequate?
5. Are the audit and internal control functions adequate?
6. Has an effective independent review function been established?
7. Are management information systems and reporting adequate?
8. Is the level of risk reasonable relative to capital and earnings levels?
9. Do the board and senior management effectively supervise this area?

PRELIMINARY REVIEW

1. Review prior examination reports, supervisory reviews, and file correspondence to identify prior rate-sensitivity concerns. Also, review internal, or third party, audits and reviews to identify any concerns or recommendations.
2. Review board or committee minutes and information packets for evidence of oversight, responsibility, routine management reports, and any identified rate sensitivity concerns.
3. Determine whether there are any recent or planned changes in strategic direction and discuss with management the implications for rate sensitivity risks.
4. Review offsite analytical reports to develop a preliminary assessment of rate sensitivity trends and risks.
5. Review the Uniform Bank Performance Report, Call Report, balance sheet, and income statement data to develop an initial rate sensitivity profile. Note common risk areas such as
    - shifts in long term assets and long term liabilities;
    - mortgage-loan exposure (direct or indirect through mortgage backed investments);
    - mortgage servicing assets;
    - significant securities depreciation;
    - structured notes;
    - fluctuations in non-maturity deposits; and
    - hedging activities, such as rate swaps, forwards, futures, options, or other derivative products.

POLICIES, PROCEDURES, AND RISK LIMITS

6. Review rate sensitivity policies. Policy guidance may be incorporated in liquidity, loan, investment, interest rate risk (IRR), or other policies, but taken as a whole, should provide sufficient guidance to management relative to the board's risk tolerances and oversight responsibilities. Policy formality and sophistication will vary, depending upon the level of the bank's risk and the complexity of its holdings and activities. In general, satisfactory policies
    - assign authority and responsibility to an individual(s) or committee for establishing and maintaining an effective IRR management program that identifies, measures, monitors, and controls IRR within board-approved risk limits;
    - identify the types of instruments and activities that may be used to manage IRR exposure;
    - provide for comprehensive measurement systems that are commensurate with the size and complexity of the institution for valuing positions and assessing performance, including procedures for updating model scenarios and underlying key assumptions;
    - require regular, detailed reporting that informs management and the board of IRR exposures;
    - outline the process and responsibility for sensitivity testing of critical model assumptions;
    - require periodic back testing of IRR projections and analysis of significant variances;
    - establish earnings and capital exposure limits commensurate with the risk tolerance of the board;
    - require management to factor IRR into broader risk management considerations and strategic decisions to ensure interrelationships between IRR and other risks are considered and addressed;
    - require the board or a designated committee to periodically review and approve the policy, risk limits, and strategies;
    - assign responsibility for authorizing policy exceptions, and require documentation of the rationale for authorizing such exceptions; and
    - provide that the asset/liability committee (ALCO), or a similar committee, has sufficient representation across major functions that influence IRR exposure.

7. Determine whether the board or a delegated committee oversees the establishment, approval, implementation, and annual review of IRR management strategies, policies, procedures, and limits (or risk tolerances).
8. Discuss IRR management processes and practices with management. Review ALCO meeting minutes and packages to evaluate the process. Potential topics for discussion include
    - lines of responsibility and authority for IRR exposure management;
    - development of IRR policies and practices;
    - adequacy of IRR measurement system used (e.g., gap, income simulation, economic value of equity);
    - assumptions used in the IRR measurement system (e.g., asset prepayments, deposit price sensitivity, decay rates, growth rates) and any adjustments to key assumptions;
    - management's understanding of the underlying analytics and methodologies of IRR models;
    - board/management understanding of model assumptions, particularly if developed by third parties;
    - strategies to manage IRR (e.g., cash flow or duration matching, altering balance sheet composition, hedging with derivatives);
    - technical expertise of staff relative to the complexity of products used and the complexity of the IRR measurement system; and,
    - board and management understanding of the specific embedded risk characteristics of the institution, (e.g., basis risk, option risk).
9. If IRR management processes include hedging with derivatives, determine whether policies outlining hedging strategies include
    - requirements for analysis of market, liquidity, credit, and operating risks;
    - requirements regarding the expertise/experience of personnel involved in implementing and monitoring derivative hedging strategies;
    - permissible strategies and types of derivative contracts;
    - risk limits for hedging activity such as position limits (gross and net), maturity parameters, and counterparty credit guidelines;
    - names of individuals authorized to initiate hedging transactions and their limits of authority;
    - requirements for monitoring hedging activity and ensuring activities fall within approved limits and lines of authority; and
    - descriptions of how management will ensure compliance with technical accounting guidance that governs hedging activity, most notably ASC Topic 815.
10. Determine whether management uses static balance sheet modeling to assess baseline IRR exposure. Refer to the 1996 Joint Agency Policy Statement on IRR and the 2010 FFIEC Advisory on IRR Management for further discussion of balance sheet modeling.
11. Determine whether management uses IRR modeling to evaluate large-scale shifts in strategies, product offerings, or significant concentrations.
12. Determine whether procedures and risk limits are reasonable relative to current economic conditions and the overall condition of the bank. Determine whether management
    - evaluates the potential effect on income and capital levels when establishing risk limits;
    - reviews limits at least annually (and more frequently if the bank's financial condition, strategic direction, or products and services are changing); and
    - considers the risks and potential rewards of adverse/favorable rate movements when establishing an IRR position or strategy.

MEASUREMENT SYSTEM CAPABILITIES

13. Determine whether the measurement system contains the functionality (and is updated as needed) to adequately assess risk exposures.
14. Determine whether the IRR measurement system captures and reports all material on- and off-balance-sheet positions. Consider the level of detail in charts of account, data input, and output reports.
15. Determine whether the system measures the

potential effect of changes in market rates on both earnings and capital.

16. Determine whether the IRR measurement system has capabilities to provide meaningful stress-test simulations applicable to the institution. Consider the following:
    - instantaneous and significant rate shocks (considering the current rate environment);
    - substantial changes in rates over time (prolonged rate shocks exceeding periods of one year);
    - changes in the relationships between key market rates (i.e., basis risk);
    - various scenarios (e.g., base case, worst case, static, dynamic); and
    - nonparallel yield curve shifts (e.g., steepened, flattened, and inverted yield curves).

ASSUMPTIONS AND DATA INPUTS

17. Assess management's process for developing and reviewing key scenarios and assumptions. Consider the institution's documentation, monitoring, and update procedures. Typical key assumptions include
    - asset prepayment speeds,
    - non-maturity deposit price sensitivities,
    - non-maturity deposit decay rates or average life, and
    - key/driver rates.
18. Review the reasonableness and support for management's key assumptions.
19. Review the institution's sensitivity analysis on key assumptions.

INTERNAL CONTROLS

20. Determine whether management established sufficient lines of authority and separation of duties, or comparable controls, over the development and use of measurement systems and monitoring tools.
21. Determine whether IRR reports are reviewed by senior management and the board at least quarterly.
22. Determine whether management complies with policy parameters and documents the reasons for variances, and any actions plans initiated. If applicable, discuss the board's oversight and approval of variances and any related mitigating actions.

AUDIT OR INDEPENDENT REVIEW

23. Determine whether management provides for an adequate audit of the IRR measurement process.
24. Determine whether the independent review includes an adequate scope (certain aspects of which may have been completed by internal audit or an external model validation). Adequate scoping generally includes an assessment of items such as the
    - adequacy of, and compliance with, policies and procedures;
    - suitability of the bank's measurement system given the size and complexity of activities;
    - appropriateness of rate scenarios used;
    - validity of risk measurement calculations; and
    - reasonableness and accuracy of assumptions and data inputs including back testing.
25. Ensure that the results of annual independent reviews are promptly reported to the board, or committee thereof. Determine whether management reviewed and reported the results of any validation performed on the IRR model used.
26. If recent reviews disclosed any deficiencies, or if back testing has shown past estimates deviated significantly from actual performance, determine whether management responses are reasonable and timely.

REPORTING AND COMMUNICATION SYSTEMS

27. Determine whether internal reports provide sufficient information for ongoing IRR management decisions and for monitoring the results of those decisions. Reports should contain sufficient detail for the board and senior management to
    - analyze IRR levels and trends and estimate the potential effect on earnings and capital;

- identify material risk exposures and sources;
- evaluate key assumptions, including interest rate forecasts, deposit behaviors, and loan prepayments;
- make pricing decisions;
- verify compliance with risk limits/policy guidelines and to monitor policy exceptions;
- assess the institution's IRR sensitivity in base-case and changing-rate scenario; and
- assess important assumptions underlying the measurement systems.

28. Determine whether interest rate risks are communicated to all relevant operational and oversight personnel.
29. Consider testing reports for accuracy by comparing results with regulatory reports and internal records.

RISK EXPOSURE CONSIDERATIONS

30. Determine the level of IRR and assess the potential effect on the institution's risk profile. Consider IRR trends that, while still within established risk tolerances, may indicate an increasing risk profile.
31. Compare the earnings projections used in the IRR measurement systems to management's budget. Determine the magnitude of any differences and the reason for the differences. Determine the extent to which management relies on IRR projections and uses them in strategic and capital planning.
32. Determine whether recent or anticipated changes or trends in the balance sheet composition alter the IRR profile relative to historical data. When significant structural changes have or are expected to occur, de-emphasize historical analysis and focus on current and forecasted balance sheet composition. Significant structural changes may include
    - major shift in the maturity (repricing) characteristics of the investment portfolio, loans, borrowings, or deposit accounts;
    - increased holdings of financial instruments such as mortgage securities, callable securities, fixed-rate residential loans, and structured notes;
    - fundamental changes in liability mix between core deposits and other funding sources;
    - unexpected changes in level or trend of securities appreciation and depreciation; and
    - adoption of, or an increase in, the volume of derivative or hedging instruments.
33. Analyze changes in the net interest margin and net operating income relative to
    - market interest rate fluctuations,
    - reliance on rate sensitive noninterest income activities (such as mortgage banking activities),
    - earnings and capital levels, and
    - strategies to manage the effect of the changes on earnings and capital.

OVERSIGHT AND RISK MITIGATION

34. Determine whether the board understands and is regularly informed about the level and trend of IRR exposure. Consider the following board responsibilities:
    - setting the bank's tolerance level for interest rate risk,
    - identifying lines of authority and responsibility for managing risk,
    - ensuring adequate resources are devoted to IRR management,
    - monitoring the overall IRR profile, and
    - ensuring that IRR is maintained at prudent levels.
35. Determine whether senior management ensures that board-approved strategies, policies, and procedures for managing IRR are appropriately executed within the designated lines of authority and responsibility. Consider the following management responsibilities:
    - implementing detailed reporting processes to inform senior management and the board of the level of IRR exposure;
    - maintaining comprehensive systems and standards for measuring IRR, valuing positions, and assessing performance, including procedures for updating IRR measurement scenarios and key underlying assumptions driving the institution's IRR analysis;

- developing and implementing procedures that translate the board's goals, objectives, and risk limits into operating standards that are understood and followed by bank personnel;
- providing sufficient staff to operate measurement systems, including back-up personnel who possess requisite technical expertise;
- establishing adequate training and development programs;
- implementing internal controls over the IRR process; and
- ensuring independent reviews and validations of the IRR program are regularly completed.

36. Determine whether historical performance indicates weakness in board and senior management oversight.
37. Determine whether the board effectively oversees and management effectively implements planned initiatives and strategies.
38. If risk limits were breached, determine what steps management took, or plans to take, to remedy, or mitigate exposures. If management decides against corrective action, determine whether such decisions are reasonable and appropriately reported and documented.

Litigation and Other Legal Matters, and Examination-Related Subsequent Events

Effective date October 2018

Section 4100.1

LITIGATION AND OTHER LEGAL MATTERS

Events or conditions arising from litigation,[1] claims, and assessments are matters within the direct knowledge and, often, control of bank management. Accordingly, management is the primary source of information about these matters.[2] Examiners ordinarily do not possess legal skills and therefore cannot make legal judgments on such information.[3] Examiners should request that bank management send a letter of inquiry to those attorneys with whom it has consulted on litigation, claims, and assessments. The letter of inquiry is the examiner's primary means of corroborating information furnished by management.

When requesting these inquiries, examiners should consider the scope of counsel's involvement with the bank. Banks may engage a number of law firms, so examiners should have the bank direct requests to both general counsel and counsel whose service is limited to particular matters. Ordinarily, inquiries should be made of all outside counsel.

In certain instances, however, examiners may be reasonably certain that some of the bank's counsels are handling only routine matters that ultimately will not have a significant effect on the bank's financial condition. In these cases, the examiner-in-charge may decide not to send letters of inquiry to those counsels.

Requests for corroboration from legal counsel should ask for information about litigation, impending litigation, claims, and contingent liabilities. For the purposes of these requests, the terms impending litigation and contingent liabilities have the following meanings:

- *Impending litigation.* Litigation threatened against the bank by a third party but not formally commenced.

- *Contingent liabilities.* Matters other than litigation or claims, which available information indicates have at least a reasonable possibility of impairing assets or increasing liabilities. Contingent liabilities should include unasserted claims or assessments.

A letter of inquiry should ask for a response both as of the examination date and as of the date of counsel's response. That date of response should be as close to the completion of the examination as practicable, yet should allow sufficient time for evaluation of responses and follow-up of nonreplies. In some cases, the examiner may wish to obtain an interim response (in addition to a final response) so that a timely preliminary evaluation of material legal matters may be made. Letters of inquiry should be sent early enough to allow them to circulate within the law firm because several attorneys may be considering legal matters for the bank. Before completing the examination, examiners should request that appropriate bank officials contact counsel who have not responded to the initial letter of inquiry.

If examination staff have reason to believe that there may be subsequent developments, the examiner should contact bank management again before submitting the report of examination. If bank management is uncooperative or regarded as incapable of supervising matters concerning litigation, or if other sensitivities mandate circumvention of bank management, then examiners should bring the matter to the attention of Federal Reserve Bank management for further communications with the bank's management and counsel, which could include direct contact with bank counsel.

EXAMINATION-RELATED SUBSEQUENT EVENTS

As a practical matter, the examination, and therefore the report of examination, is as of a

1. Legal risk arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a financial institution.

2. In limited circumstances, a bank director who is not an officer of the bank may have direct knowledge and control of legal information, usually when the director's primary occupation is as an attorney. Management in these rare instances may have limited knowledge and control of legal information.

3. Appropriate examination staff should notify the enforcement section of Board Legal of any investigations or other legal actions being conducted by governmental regulators or criminal prosecutors against the bank when such information is ascertained during the examination process.

stated date. However, events or transactions sometimes occur, subsequent to the date of examination, but before the date the report of examination is submitted to the Reserve Bank, that may have a significant effect on the soundness of a bank. Such events and transactions are referred to as ''subsequent events'' and may be of two types.

One type includes those events or transactions that provide additional evidence about conditions that existed at the examination date. Examples of this type are the bankruptcy of a significant borrower or the resolution of outstanding litigation.

The second type includes those events that provide evidence about conditions that did not exist at the date of examination but that arose subsequently. An example of that type of event would be new litigation arising subsequent to the examination date but before submission of the examination report.

All information that becomes available before the submission of the report of examination should be used by examiners in the evaluation of the bank. Accordingly, all events or transactions that either significantly affect or have the potential to significantly affect the soundness of the bank should be reflected in the report of examination, regardless of whether they occurred before or subsequent to the examination date.

Litigation and Other Legal Matters, and Examination-Related Subsequent Events

Examination Objectives

Effective date October 2018

Section 4100.2

1. To determine whether any events or transactions have occurred subsequent to the examination date that have had or may have a significant impact on the present or future soundness of the bank or on the conclusions expressed in the report of examination.
2. To determine the adequacy of risk management practices surrounding litigation and other legal matters.
3. To determine the effect of legal counsel's evaluation of litigation, impending litigation, claims, and contingent liabilities on the examiner's overall conclusion regarding the soundness of the bank.

1. Read minutes of all meetings of stockholders, directors, and appropriate committees (investment, loans, etc.).
   a. Ascertain from officials of the bank whether minutes of all such meetings subsequent to the examination date are set forth in the minute book.
   b. As to meetings for which minutes have not been prepared at the date of the review, inquire directly of persons present at the meetings and, preferably, of the person charged with the responsibility of preparing the minutes, concerning matters dealt with at such meetings.
2. If specific violations of law or areas of weakness have been reported to management earlier in the examination, determine the extent to which management has proceeded toward corrective action.
3. Obtain from the bank officer responsible for legal matters a listing of impending or threatened litigation. For each item, the following information should be included:
   a. nature of the litigation
   b. progress of case to date
   c. how management is responding or intends to respond to the litigation
   d. an evaluation of the likelihood of an unfavorable outcome and an estimate, if one can be made, of the amount or range of potential loss
4. Obtain from the bank officer responsible for legal matters a listing of unasserted claims or assessments management considers will probably be asserted and which, if asserted, would have at least a reasonable possibility of an unfavorable outcome. For each item, the following information should be included:
   a. nature of the matter
   b. how management intends to respond if the claim is asserted
   c. possible exposure if the claim is asserted
5. Obtain from management a listing of attorneys and legal firms to whom litigation and related matters have been referred. Also, obtain a listing of any litigation noted in the newest review done by internal or external auditors from the examiner assigned internal control, and determine that corrections have been accomplished.
6. Review bills supporting major charges to the general ledger expenses account(s) for legal services as a test of the completeness of the list supplied by the bank.
7. Request that management incorporate information obtained in above steps in a letter to the bank's legal counsel for corroboration.
8. Evaluate management's listing of litigation, unasserted claims and assessments, and counsel's replies for the effect on the financial condition of the bank, giving appropriate consideration to any insurance coverage.
9. Obtain and review copies of any subsequent interim financial statements. Examples of such statements are—
   a. published reports sent to shareholders or others;
   b. reports submitted to the board of directors by internal auditors, external auditors, or management;
   c. statements of condition; and
   d. income statements.
      - Inquire as to whether interim statements obtained were prepared on the same basis as that used for the statements as of the examination date. If not, request proper adjustments to the interim statements.
      - Compare the interim financial statements, especially income statements, with similar statements for the corresponding period in the prior year and to budgets, profit plans, etc., for the current period, if such are available.
      - Obtain from management satisfactory explanations for any unusual items or significant fluctuations noted.
10. Make inquiries of and hold discussions with officers and other executives who have responsibility for the following matters:
    a. changes in credit lines or transactions with officers, directors, controlling shareholders, affiliated bank holding companies, affiliates of an affiliated holding company, or their interests
    b. changes in significant accounting policies
    c. changes in senior officers
    d. any event or combination of events which

have had or could have a material adverse effect on the bank's financial condition, including liquidity, or results of operation, such as the default of a bond issue in which the bank has substantial holdings or the filing of bankruptcy by a major borrower

e. commencement or discontinuance of services not requiring prior approval
f. execution of significant contracts, such as for employment, leases, pension, or other fringe benefit programs
g. significant new contingent liabilities or commitments other than those referred to above
h. significant changes in assets which may not be evident from the review of subsequent interim financial statements, such as a shift in the amount of loans or investments in special categories, or unusal adjustments made in or after the subsequent interim financial statements reviewed in connection with the previous procedure

11. Distribute information obtained in the previous steps to the appropriate examiners. Notify the enforcement section of Board Legal of any investigations or other legal actions being conducted by governmental regulators or criminal prosecutors against the bank when such information is ascertained during the examination process
12. Make additional inquiries or perform such procedures as considered necessary and appropriate to dispose of questions that arose in the course of the preceding procedures, inquiries, and discussions.
13. If, as a result of performing the above procedures, information is obtained that has a significant impact on the evaluation of the soundness of the bank, extend the appropriate examination procedures so that sufficient evidence is reviewed and documented in the workpapers to support the conclusions reached.
14. Prepare comments for the examination report on any events or transaction noted which may have a material effect on the soundness of the bank.
15. Update the workpapers with any information that will facilitate future examinations.

INTRODUCTION

Off-balance-sheet credit activities have been one of the fastest growing areas of banking activity. Although these activities may not be reflected on the balance sheet, they must be thoroughly reviewed because they can expose the bank to contingent liabilities. Contingent liabilities are financial obligations of a bank that are dependent on future events or actions of another party.

The purpose of this section is to provide a concise reference for contingent liabilities that arise from off-balance-sheet credit activities (for example, loan commitments and letters of credit). This section will also include some discussion of other contingent liabilities, which arise from asset sales and other off-balance-sheet activities. Activities such as trusts, securities clearance, securities brokerage, and corporate management advisory services involve significant operational and fiduciary risks and require specialized examination procedures. Consult section 6010, "Other Types of Examinations," in this manual for further information about these activities.

Derivatives are also not covered in this section. The acquisition and management of derivatives for the bank's own account are covered in detail in sections 2020 and 4090, "Acquisition and Management of Nontrading Securities and Derivative Instruments" and "Interest-Rate Risk Management" of this manual. The *Trading Activities Manual* provides more specific guidance for the examination of banks that are involved in derivatives trading and customer accommodation activities.

Risks associated with contingent liabilities may ultimately result in charges against capital. As a result, full-scope examinations will include an analysis of these risks. Each of the major components of the examination—capital, asset quality, management, liquidity, and earnings—incorporates an assessment of the risks associated with off-balance-sheet credit activities. While it is impossible to enumerate all of the types and characteristics of contingent liabilities here, some of the more common ones are discussed in this section. In all cases, the examiner's overall objectives are to assess the potential impact of these contingent liabilities on the financial condition of the bank, to ascertain the likelihood that such contingencies may ultimately result in losses to the bank, to ensure that management has appropriate systems to identify and control contingent liabilities, and to ensure compliance with all applicable laws, regulations, and statements of regulatory policy.

OFF-BALANCE-SHEET LENDING ACTIVITIES

In reviewing individual credit lines, all of a customer's borrowing arrangements with the bank (for example, direct loans, letters of credit, and loan commitments) should be considered. The factors analyzed in evaluating a direct loan (financial performance, ability and willingness to pay, collateral protection, and future prospects) are applicable to the review of off-balance-sheet lending arrangements. When analyzing these activities, however, examiners should evaluate the probability of draws under the bank's off-balance-sheet lending arrangements with its customers and should evaluate whether the allowance for loan and lease losses adequately reflects the associated risks. Consideration should also be given to compliance with laws and regulations. Refer to section 2040, "Loan Portfolio Management," of this manual for further details.

Loan Commitments

A formal loan commitment is a written agreement signed by the borrower and the lender that details the terms and conditions under which a loan, up to a specified amount, will be made. Unlike a standby letter of credit, which commits the bank to satisfying its customer's obligation to a third party, a loan commitment involves only the bank and its customer. The commitment will have an expiration date and, in exchange for agreeing to make the accommodation, the bank often requires the customer to pay a fee and/or maintain a stipulated compensating balance.

Some commitments, such as a working capital line, revolving credit facility, or a term loan facility, are expected to be used. Other commitments, such as back-up lines of credit for commercial paper issuance, involve usage that is not anticipated unless the customer is unable to retire or roll over the issue at maturity.

Lines of Credit

A line of credit expresses to the customer, usually by letter, a bank's willingness to lend up to a certain amount over a specified timeframe. These lines of credit are disclosed to the customer and are referred to as "advised" or "confirmed" lines. In contrast, "guidance" lines (also referred to as internal guidance lines) are not disclosed to the customer. "Guidance" lines of credit are formally approved like any other loans or commitments and are established to aid the loan officer who is servicing an account act quickly to an unexpected request for funds. Many lines of credit may be cancelled if the customer's financial condition deteriorates; others are simply subject to cancellation at the option of the issuer, such as "guidance" lines and other nonbinding agreements. Lines of credit usually require periodic or annual borrowing cleanups. Not adhering to cleanup provisions is a well-defined weakness.

Disagreements may arise as to what constitutes a legally binding commitment. A bank's own descriptive terminology alone may not always be the best guideline. For example, a credit arrangement could be referred to as a revocable line of credit but, at the same time, it may be a legally binding commitment to lend—especially if consideration has been given by the customer for the bank's promise to lend and if the terms of the agreement between the parties result in a contract. Therefore, management of the bank should properly distinguish its legally binding loan commitments from its revocable loan commitments. Proper documentation will help ensure that the bank's position is defensible if legal action becomes necessary to cancel a loan commitment.

Some lending agreements contain a "material adverse change" (MAC) clause, which is intended to allow the bank to terminate the commitment or line of credit if the customer's financial condition deteriorates. This clause may apply to the continuing financial condition of guarantors. The extent to which MAC clauses are enforceable depends on several factors, including whether a legally binding relationship remains despite specific financial covenants that are violated. Some documents make only a vague reference to a borrower's responsibility for maintaining a satisfactory financial condition. Although the enforceability of MAC clauses may be subject to some uncertainty, such clauses may provide the bank with leverage in negotiations with the customer over such issues as requests for additional collateral and/or personal guarantees.

A bank cannot always routinely determine whether funding of a commitment or line of credit will be required; therefore, the examiner must always subject the line of credit to careful analysis. A MAC clause could allow the bank to refuse funding to a financially troubled borrower; a default in other contract covenants could cause the termination of the commitment or line of credit. Some banks might strictly enforce the terms of a credit arrangement and refuse funding if any of the covenants are broken. Other banks take a more accommodating approach and will continue to make advances unless the customer files for bankruptcy. In the final analysis, the procedures normally followed by the bank in honoring or terminating a contingent lending agreement are important in the examiner's overall evaluation of the credit risk.

Risk Management for Loan Commitments and Lines of Credit

The primary risk inherent in any future extension of credit is that the condition of the borrower may change between the issuing of the commitment and its funding. However, commitments may also entail liquidity and interest-rate risk.

Examiners should evaluate anticipated drawdowns of an issuing bank's loan commitments and lines of credit relative to the bank's anticipated funding sources. A draw under lines of credit may be in the form of a letter of credit issued on the borrower's behalf. Such letters of credit share the same collateral as the line of credit, and the issuance of the letter of credit uses availability under the line. At each examination, the draws that are anticipated for unused commitments and advised lines of credit should be estimated. If the amount of unfunded commitments is large relative to the bank's liquidity position, further analysis is suggested to determine whether borrowed funds will have to be used and, if so, the amount and sources of such funds. Concerns and comments should be noted on the Liquidity/Funds Management page in the report of examination. Also, loan commitments are to be reported on the commitments and contingencies schedule in the report of exami-

nation. For further information, refer to sections 4020, 4090, and 6000, ‘‘Asset/Liability Management,’’ ‘‘Interest-Rate Risk Management,’’ and ‘‘Instructions for the Report of Examination,’’ in this manual.

LETTERS OF CREDIT

A letter of credit substitutes the credit capacity of a financial institution for that of an individual or a corporation. The concept of substituting one obligor’s financial standing for another party’s financial standing has been used in financing the international shipment of merchandise for centuries (imports and exports). Today, letters of credit are also used in a wide variety of other commercial financing transactions, such as guaranteeing obligations involving the private placement of securities and ensuring payment in the event of nonperformance of an obligated party. In addition, letters of credit are used to secure the guarantees of principals in real estate development loans. For additional information on letters of credit, see section 7080, ‘‘International—Letters of Credit,’’ in this manual.

Elements of a Letter of Credit

A letter of credit should contain the following elements:

- a conspicuous statement that the document is a letter of credit
- a specified expiration date or a definite term and an amount
- an obligation of the issuer to pay that is solely dependent on the presentation of conforming documents as specified in the letter of credit and not on the factual performance or nonperformance by the parties to the underlying transaction
- an unqualified obligation of the account party to reimburse the issuer for payments made under the letter of credit

A letter of credit involves at least three parties and is three separate and distinct contracts:

- a contract between the account party and the beneficiary under which the account party has an obligation of payment or performance
- a contract between the account party and the issuer of the letter of credit (The issuer is the party obligated to pay when the terms of the letter of credit are satisfied. The account party agrees to reimburse the issuer for any payments made.)
- a contract between the issuer and the beneficiary, whereby the issuer agrees to pay the beneficiary in compliance with the terms and conditions of the letter

Policies and Procedures

Maintaining adequate written policies and procedures and monitoring letters of credit activities are part of the fiduciary and oversight responsibilities of the board of directors. Generally, policies and procedures governing the institution’s issuance of letters of credit are contained in a section of the loan policy manual.

The letter of credit policy should thoroughly explain the institution’s procedures in issuing both commercial letters of credit and standby letters of credit. The policy should outline desirable and undesirable issuances, designate persons authorized to issue letters of credit and their corresponding loan authority, and define the recordkeeping and documentation requirements including the need to establish separate files for each issuance.

If several lending departments issue letters of credit, the policy should explicitly assign responsibility for file maintenance and recordkeeping. A separate file containing an exact copy of each outstanding letter of credit and all the supporting documentation that the underwriter used in deciding to issue the letter should be included in the file. This documentation should be the same as the financial documentation used for originating any other form of credit, which includes current financial statements, current income statements, purpose of the letter of credit, collateral-security documentation, proof-of-lien position, borrowing authorization, all correspondence, and officers’ memoranda.

Documentation

In addition, the file must contain the documentation associated with any disbursements or payments made. For a commercial letter of credit, these documents may include—

- the draft (sometimes called the bill of exchange), which is the demand for payment;
- the commercial invoice, a document describing the goods being shipped (prepared by the seller and signed by the buyer);
- the bill of lading, which documents that shipment of the goods has taken place and gives the issuer an interest in the goods in the event the account party defaults;
- customs documentation that verifies that all required duties have been paid;
- the insurance certificate, which provides evidence that the seller has procured insurance;
- the consular documents, which state that the shipment of goods satisfies the import/export regulations; and
- the certificates of origin and inspection, which state that the goods originated in a specified country to guard against the substitution of second-quality merchandise.

The documents associated with standby letters of credit are far less complicated than those for commercial letters of credit. Often no document is necessary to support the beneficiary's draw upon a standby letter of credit. This is what is referred to as a clean standby letter of credit and should be discouraged due to the possible legal expense of defending any action taken in honoring or dishonoring a draw without specific documentary requirements. At a minimum, standby letters of credit should require a beneficiary's certificate asserting that the account party has not performed according to the contract or has defaulted on the obligation, as well as a copy of the contract between the account party and beneficiary.

Accounting Issues

Since letters of credit represent a contingent liability to the issuing institution, they must be disclosed in the financial statements in accordance with generally accepted accounting principles (GAAP). The Financial Accounting Standards Board has stipulated in its Statement of Financial Accounting Standard No. 5 that the nature and the amount of a standby letter of credit must be disclosed in the institution's financial statement. Commercial letters of credit and standby letters of credit should be accounted for on the balance sheet as liabilities if it is probable that the bank will disburse funds, and if the amount of the funding is determinable. Most standby letters of credit will not be recorded as a liability. However, their existence will be disclosed in the footnotes to the financial statements.

Benefits of Letters of Credit

Both the customer and the financial institution can benefit from letters of credit. Through the use of a letter of credit, a customer can often obtain a less expensive source of funds than would be possible through direct financing from the institution. For example, the customer may be able to take advantage of a seller's credit terms with the backing of a letter of credit to substantiate the customer's credit capacity. The institution receives a fee for providing the service. In addition, the institution hopes to build a better working relationship with its customers, who may generate or refer other profitable business.

Revocable or Irrevocable

Letters of credit can be issued as either revocable or irrevocable. The revocable letter of credit is rarely used because it may be amended or canceled by the issuer without the consent of the other parties. Most letters of credit are issued as irrevocable with a stipulation that no changes may be made to the original terms without the full consent of all parties.

Risks in Issuing Letters of Credit

A financial institution must be aware of the credit risks that are associated with letters of credit and must issue letters of credit only when its resources are adequate. Although letters of credit are not originally made as loans, they may lead to loans if the account party cannot meet its obligations. Therefore, the institution must implement the same prudent underwriting guidelines for letters of credit as for other extensions of commercial credit. Refer to section 2080, "Commercial Loans," in this manual for further details.

The importance of adequate documentation cannot be overemphasized. Commercial letters of credit are part of a continuous flow of

transactions evolving from letters of credit to sight drafts to acceptances. Repayment may depend on the eventual sale of the goods involved; however, the goods may not provide any collateral protection. Thus, proper handling and accuracy of the required documents are of primary concern. Letters of credit are frequently issued via tested telex, which verifies the authenticity of the sender (usually another bank). No institution should honor a letter of credit presented by a beneficiary without first confirming its authenticity.

Commercial letters of credit involving imports must be considered unsecured until the goods have passed customs, the security documents specified in the letter of credit have been presented, and the goods have been verified and controlled.

Letters of credit are subject to the risk of fraud perpetrated by customers, beneficiaries, or insiders of the issuing institution. Moreover, standby letters of credit can be used by officers or directors as a vehicle for obtaining credit at another institution. It is important to note that Regulation O requirements apply to standby letters of credit.

Consequently, letters of credit should be issued under the same strict internal controls as any other extension of credit. Such controls include a requirement of dual or multilevel authorizations and the segregation of the issuing, recordkeeping, acceptance, and payment functions.

Risks in Honoring Letters of Credit

The honoring of another institution's letter of credit or acceptance requires strict verification procedures as well as dual authorization by the honoring financial institution. Reasons for strict procedures and authorizations are numerous. The issuer may be unable or unwilling to honor a letter of credit or standby letter of credit, claiming that the document is fraudulent or a forgery or that the signer was unauthorized. Before honoring any other institution's letter of credit, a bank should confirm in writing that the letter of credit is valid and will be honored under specified conditions. Agreements with issuers for accepting letters of credit issued by tested telex should provide specific conditions under which they will be honored.

To minimize risks of loss, compliance with the conditions outlined within the letter of credit must be strict—not merely substantial. Testing of LOCs should involve two or more persons through dual authorization or segregation of duties to prevent fraud by employees in this process.

Uniform Commercial Code

Both the issuer and the beneficiary of letters of credit are obligated to conform to a uniform set of rules governed by article 5 of the Uniform Commercial Code (UCC). These rules are referenced in the Uniform Customs and Practice for Documentary Credits (UCP). The UCC is a set of articles governing commercial transactions adopted by various states, whereas the UCP encompasses all of the international guidelines for trading goods and services. Local laws and customs vary and must be followed under advice of counsel.

TYPES OF LETTERS OF CREDIT

There are two major types of letters of credit: the commercial letter of credit, also referred to as a trade letter of credit, and the standby letter of credit. Banks have significantly increased their issuances of letters of credit, particularly standby letters. A contributing factor to this significant increase is that by issuing letters of credit, an institution can increase its earnings without disbursing funds and increasing total assets. The institution charges a fee for the risk of default or nonperformance by the customer, thereby increasing the bank's return on average assets. It is important for examiners to be concerned with the elements of risk that are present in the institution's practices regarding the issuance of letters of credit. Examiners should then assess the institution's system of controls that can mitigate the risks (including staff experience, proper documentation, and the quality of underwriting). The standards for issuing letters of credit should be no less stringent than the standards for making a loan. Likewise, the letter-of-credit portfolio requires a review as thorough as the lending review. A default or nonperformance by the account party of a letter of credit will have the same impact as a default on a loan.

Commercial Letters of Credit

The commercial letter of credit (LOC) is commonly used as a means of financing the sale of goods between a buyer and seller. Generally, a seller will contract with a buyer on an open-account basis, whereby the seller ships the goods to the buyer and submits an invoice. To avoid the risk of nonpayment, the seller may require the buyer to provide a commercial letter of credit. To satisfy the requirement, the buyer applies for a letter of credit at a financial institution. If approved, the letter of credit would contain specified terms and conditions in favor of the seller (beneficiary), and the buyer (account party) would agree to reimburse the financial institution for payments drawn against the letter. The commercial letter of credit can be used to finance one shipment or multiple shipments of goods. Once documents that provide evidence that the goods have been shipped in accordance with the terms of the letter of credit are received, the seller can draw against the issued letter of credit through a documentary draft or a documentary demand for payment. The institution honors the draft, and the buyer incurs an obligation to reimburse the institution.

Letters of credit can be secured by cash deposits, a lien on the shipped goods or other inventory, accounts receivable, or other forms of collateral. Commercial letters of credit ''sold for cash'' (that is, secured by cash deposits) pose very little risk to a bank as long as the bank, before making payment on the draft, ensures that the beneficiary provides the proper documents. If credit is extended to pay for the goods, the subsequent loan presents the same credit risks associated with any other similar loan.

Standby Letters of Credit

The standby letter of credit (SBLOC) is an irrevocable commitment on the part of the issuing institution to make payment to a designated beneficiary if the institution's customer, the account party, defaults on an obligation. The SBLOC differs from the commercial letter of credit because it is not dependent on the movement of goods. While the commercial letter of credit eliminates the beneficiary's risk of nonpayment under the contract of sale, the SBLOC eliminates the financial risks resulting from nonperformance under a contract. The SBLOC, in effect, enhances the credit standing of the bank's customer.

SBLOCs may be financially oriented (financial SBLOCs), whereby an account party agrees to make payment to the beneficiary, or SBLOCs may be service-oriented (performance SBLOCs), whereby the financial institution guarantees to make payment if its customer fails to perform a nonfinancial contractual obligation.

Financial SBLOCs

Financial SBLOCs are often used to back direct financial obligations such as commercial paper, tax-exempt securities, or the margin requirements of exchanges. For example, if the bank's customer issues commercial paper supported by an SBLOC, and the bank's customer is unable to repay the commercial paper at maturity, the holder of the commercial paper may request the bank to make payment. Upon receipt of the request, the bank would repay the holders of the commercial paper and account for the payment as a loan to the customer under the letter of credit. Because of this irrevocable commitment, the bank has, in effect, directly substituted its credit for that of its customer upon the issuance of the SBLOC; consequently, the SBLOC has become a credit enhancement for the customer.

Performance SBLOCs

Performance SBLOCs are generally transaction-specific commitments that the issuer will make payment if the bank's customer fails to perform a nonfinancial contractual obligation, such as to ship a product or provide a service. Performance SBLOCs are often used to guarantee bid or performance bonds. Through a performance SBLOC, the bank provides a guaranty of funds to complete a project if the account party does not perform under the contract. In contrast to the financial SBLOC, the bank's irrevocable commitment provides liquidity to the obligor and not directly to a third-party beneficiary.

Unlike a commercial letter of credit, a demand for payment against an SBLOC is generally an indication that something is wrong. The nonperformance or default that triggers payment under the SBLOC often signals the financial weakness of the customer, whereas payment under a commercial letter of credit suggests that

the account party is conducting its business as usual. Standby letters of credit can be either unsecured or secured by a deposit or other form of collateral.

Uses

The uses of standby letters of credit are practically unlimited. The more common areas of use include the following.

Financing Real Estate Development. A mortgagee will condition its loan commitment upon a cash contribution to a project by the developers. Although the lender insists that the developers have some equity in the project, the developer may not have funds available as they are tied up in other projects. The parties often use the letter of credit to satisfy the requirement for equity without the need for a cash deposit.

Fulfilling Municipal Regulations. Most municipalities require some form of a performance bond to ensure that infrastructure improvements, such as buildings, roads, and utility services, are completed. Because the bonding companies generally required a letter of credit as collateral for their bond, developers began offering the SBLOC to the municipality as a substitute. The SBLOC is probably more common than the performance bond. The SBLOC provides the municipality the guaranty of funds to complete necessary improvements if the developer does not perform as required.

Securing Notes. A lender will sometimes ask its obligor to secure the balance of a promissory note with an SBLOC issued by another bank.

Ensuring Performance. The standby letter of credit is similar to a performance bond. Often the seller of goods will have the borrower obtain a commercial letter of credit to ensure payment; simultaneously, the buyer will have the seller obtain a standby letter of credit to ensure that the goods are delivered when agreed and in acceptable condition.

Guaranteeing Securities. The standby letter of credit guarantees obligations involving the private placement of securities, such as revenue and development bonds. If an SBLOC secures against default, such paper will generally have a higher rating and bear a lower rate of interest. An SBLOC could also be used as a credit enhancer for packaging retail loans for public sale. The use of an SBLOC in this situation typically carries minimal overall risk because the packaging institution normally sets aside a contingent reserve for losses. However, if the reserve is inadequate, the SBLOC should be reviewed for possible classification.

SBLOCs Issued as Surety for Revenue Bonds

SBLOCs may be issued in conjunction with the development of a property that is financed with tax-free or general revenue bonds. In these transactions, a municipal agency—typically, a local housing authority or regional development authority—sells bonds to investors in order to finance the development of a specific project. Once the bonds are issued, the proceeds are placed with a trustee and then loaned at less than market rates to the developer of the project. The below-market-rate loan that is granted to the developer enables the municipal agency to encourage development without expending tax dollars. The municipal agency has no liability; the bond investors only have recourse against the specific project. If the bonds are exempt from federal taxation, they will generally carry a below-market interest rate. If the bonds are not tax free—and some municipal bonds are not tax free—they will carry a market rate of interest.

Because the bonds are secured only by the project, an SBLOC is typically obtained by the beneficiary (in this example, the municipal agency) from a financial institution to provide additional security to the bondholders. The SBLOC is usually for an amount greater than the face amount of the bonds, so the bondholders' accrued interest between interest payment dates is usually secured. The bank generally secures its SBLOC with a lien that is subordinate to the authority's or trustees' lien against the property and the personal guarantees of the principal. Underwriting standards and credit analysis for SBLOCs should mirror those employed for direct loans.

The trustee receives periodic payments from the developer and then pays the bondholders their periodic interest payments and also pays the financial institution its letter-of-credit fee. In the event of a default by the developer, the trustee will draw upon the SBLOC to repay the

bondholders. If such a default occurs, the issuing financial institution assumes the role of the lender for the project.

The structure of the transaction requires the bank issuing the SBLOC to assume virtually all of the risk. Because the purpose of these bonds is to encourage development, financially marginal projects, which would not be feasible under conventional financing, are often financed in this manner. The primary underwriting consideration is the ability of the securing property to service the debt. The debt-service-coverage calculations should include both the tax-free rate, if applicable, obtained through the revenue bonds and market interest rates. The operations of the securing property should also be monitored on an ongoing basis. If new construction is involved, the progress should be monitored and any cost overruns should be identified and addressed.

Renewal of SBLOCs

Although most SBLOCs contain periodic renewal features, the examiner must be aware that the bank cannot relieve itself from liability simply by choosing not to renew the SBLOC. Virtually all of the bond issues require a notice of nonrenewal before the expiration of the SBLOC. If such notice is received by the trustee, the trustee normally considers the notice an event of default and draws against the existing SBLOC. The bank should protect itself, therefore, by continuously monitoring both the project and the status of the bonds. Documentation should be maintained in the bank's file to substantiate the property's occupancy, its cashflow position, and the status of the bonds. In addition to the current status of interest payments, any requirements for a sinking fund that are contained in the bond indenture should also be monitored.

Some letters of credit are automatically renewable unless the issuing bank gives the beneficiary prior notice (usually 30 days). These letters of credit represent some additional risk because of the notification requirement placed on the bank. As noted above, proper monitoring and timely follow-up are imperative to minimize risk.

Without the benefit of a substantial guarantor or equity in the collateral, these SBLOCs present more than normal risk of loss. If the SBLOC is converted into an extension of credit, the loan will likely be classified substandard or worse. Protection against loss may be provided by a long-term lease from a major tenant of an industrial property or a lease from a housing authority with a governmental funding commitment or guaranty.

Classification of SBLOCs

It may be appropriate to adversely classify an SBLOC if draws under the SBLOC are probable and a well-defined credit weakness exists. For example, deterioration of the financial standing of the account party could jeopardize performance under the letter of credit and result in the requirement of payment to the beneficiary. Such a payment would result in a loan to the account party and could result in a collection problem, especially if the SBLOC was unsecured. If payment is probable and the account party does not have the ability to repay the institution, an adverse classification is warranted. FASB 5 requires that if a loss contingency is probable and can be reasonably estimated, a charge to income must be accrued. Refer to section 2060, "Classification of Credits," in this manual for procedures on SBLOC classification.

BANKER'S ACCEPTANCES

When the beneficiary presents a draft to the issuer in compliance with the terms of a commercial letter of credit, the method of honoring the draft is acceptance. The issuer will stamp the word "accepted" across the face of the draft, which makes the instrument negotiable. Thus, the institution upon which the draft is drawn converts what was originally an order to pay into an unconditional promise to pay. Depending on the terms specified in the letter of credit, payment of the draft can vary from sight to 180 days. There is a ready market for these instruments, because payment must be made at maturity by the accepting institution, whether or not it is reimbursed by its customer. These acceptances are readily negotiable, and a beneficiary may sell accepted time drafts to other financial institutions at a discount. Acceptances are governed by article 3 of the UCC, and any rights the parties have under acceptance are subject to the rules of that article. For further discussion of banker's acceptances, see section 7060, "International—Banker's Accep-

tances,'' and the Instructions for the Preparation of the Report of Condition and Income.

Participations in Banker's Acceptances

The following discussion refers to the roles of accepting and endorsing banks in banker's acceptances. It does not apply to banks purchasing other banks' acceptances for investment purposes. Banker's acceptances may represent either a direct or contingent liability of the bank. If the acceptance is created by the bank, it constitutes a direct liability that must be paid on a specified future date. The acceptance is also an on-balance-sheet, recognized liability. If a bank participates in the funding risk of an acceptance created by another bank, the liability is contingent and the item is carried off-balance-sheet. The financial strength and repayment ability of the accepting bank should be considered in analyzing the amount of risk associated with these contingent liabilities.

Participations in acceptances conveyed to others by the accepting bank include transactions that provide for the other party to the participation to pay the amount of its participated share to the accepting bank at the maturity of the acceptance, whether or not the account party defaults. Participations in acceptances acquired by the nonaccepting bank include transactions that provide for the nonaccepting bank to pay the amount of its participated share to the accepting bank at the maturity of the acceptance, whether or not the account party defaults.

Call Report Treatment

For regulatory reporting purposes, the existence of such participations is not to be recorded on the balance sheet. Rather, both the accepting bank conveying the participation to others and the bank acquiring the participation from the accepting bank must report the amounts of such participations in the appropriate item in Schedule RC-L, Commitments and Contingencies. (The amount of participations in acceptances reported in Schedule RC-L by a member bank may differ from the amount of such participations that enter into the calculation of the bank's acceptances to be counted toward its acceptance limit imposed by section 13 of the Federal Reserve Act (12 USC 372). These differences are mainly attributable to participations in ineligible acceptances, to participations with ''uncovered'' institutions, and to participations that do not conform to the minimum requirements set forth in 12 CFR 250.163.)

NOTE-ISSUANCE AND REVOLVING UNDERWRITING CREDIT FACILITIES

The first note-issuance facility (NIF) was introduced in 1981. A NIF is a medium-term (five- to seven-year) arrangement under which a borrower can issue short-term paper. The paper is issued on a revolving basis, with maturities ranging from as low as seven days to up to one year. Underwriters are committed either to purchasing any unsold notes or to providing standby credit. Bank borrowing usually involves commercial paper consisting of short-term certificates of deposit and, for nonbank borrowers, generally promissory notes (Euronotes). Although NIF is the most common term used for this type of arrangement, other terms include the revolving underwriting facility (RUF) and the standby note-issuance facility (SNIF).

Another type of facility, a RUF, was introduced in 1982. A RUF is a medium-term revolving commitment to guarantee the overseas sale of short-term negotiable promissory notes (usually a fixed-spread over LIBOR) issued by the borrower at or below a predetermined interest rate. RUFs separate the roles of the medium-term risk-taker from the funding institutions (the short-term investors). RUFs and NIFs allow access to capital sources at interest rates considerably below conventional financing rates. The savings in interest cost are derived because the borrower obtains the lower interest costs prevailing in the short-term markets, while still retaining the security of longer term financing commitments. The notes issued under RUFs are attractive for institutional investors since they permit greater diversification of risk than the certificates of deposit of only one bank. Underwriters favor them because their commitments do not appear on the statement of financial condition. RUFs are usually structured for periods of four to seven years.

A RUF differs from a NIF in that it separates the functions of underwriting and distribution. With a RUF, the lead bank (manager or arranger)

acts as the only placing agent. The arranger retains total control over the placing of the notes.

NIFs and RUFs are discussed further in the *Bank Holding Company Supervision Manual*.

GUARANTEES ISSUED

State member banks and foreign branches of U.S. banks are allowed to issue guarantees or sureties under certain circumstances. Such guarantees are to be reported as contingent liabilities in Schedule RC-L. Refer to section 7090, ''International—Guarantees Issued,'' of this manual and to the call report instructions for further information.

ASSET SALES

The term ''asset sales,'' in the following context, encompasses the range of activities from the sale of whole loans to the sale of securities representing interests in pools of loans. Asset-sales programs entail establishing both a portfolio of assets that are structured to be easily salable and a distribution network to sell the assets. Most large banks have expended great effort in developing structures and standard procedures to streamline asset-sale transactions and continue to do so.

Asset sales, if done properly, can have a legitimate role in a bank's overall asset and liability management, and can contribute to the efficient functioning of the financial system. In addition, these activities can assist a bank in diversifying its risks and improving its liquidity.

The benefits of a qualifying sale transaction are numerous. In particular, the sale of a loan reduces capital requirements. The treatment also enhances net income, assuming that the loan was sold for a profit.

Banks' involvement in commercial loan sales and in public issuance of mortgage and asset-backed securities has grown tremendously over the last decade. Banks are important both as buyers and sellers of whole loans, loan participations, and asset-backed securities. Banks also play important roles in servicing consumer receivables and mortgages backing securities and in providing credit enhancement to originators of primarily asset-backed securities.

Both whole loans and portions of loans are sold. Banks sell portions of loans through participation arrangements and syndication agreements.

Participations

A loan participation is a sharing or selling of ownership interests in a loan between two or more financial institutions. Normally, a lead bank originates the loan and sells ownership interests to one or more participating banks at the time the loan is closed. The lead bank (originating bank) normally retains a partial interest in the loan, holds all loan documentation in its own name, services the loan, and deals directly with the customer for the benefit of all participants. Properly structured, loan participations allow selling banks to accommodate large loan requests that would otherwise exceed lending limits, to diversify risk, and to improve liquidity by obtaining additional loanable funds. Participating banks are able to compensate for low local demand for loans or invest in large loans without their servicing burdens and origination costs. If not appropriately structured and documented, however, a loan participation can present unwarranted risks to both the seller and purchaser of the loan. Examiners should determine the nature and adequacy of the participation arrangement and should analyze the credit quality of the loan. For further information on participations, refer to section 2040, ''Loan Portfolio Management,'' in this manual.

Syndication

A syndication is an arrangement in which two or more banks lend directly to the same borrower pursuant to one loan agreement. Each bank in the syndicate is a party to the loan agreement and receives a note from the borrower evidencing the borrower's debt to that bank. Each participant in the syndicate, including the lead bank, records its own share of the participated loan. Consequently, the recourse issues and contingent liabilities encountered in a loan participation involving syndication are not normally an issue. However, many banks involved in syndicated transactions will sell some of their allotment of the facility through subparticipations. These subparticipations should

be reviewed in the same manner as any other participation arrangement.

Asset Securitization

Banks have long been involved with asset-backed securities, both as investors in these securities and as sellers of assets within the context of the securitization process. In recent years, banks have increased their participation in the long-established market for those securities that are backed by residential mortgage loans. They have also expanded their securitizing activities to other types of assets, including credit card receivables, automobile loans, boat loans, commercial real estate loans, student loans, nonperforming loans, and lease receivables. See section 4030, "Asset Securitization," for a detailed discussion of the securitization process.

Risks

Assets sold without recourse are generally not a contingent liability, and the bank should reflect on its books only that portion of the assets it has retained. In some instances, however, participations must be repurchased to facilitate ultimate collection. For example, a bank may sell the portion of a loan that is guaranteed by the Small Business Administration (SBA) and retain the unguaranteed portion and the responsibility for servicing the loan. In the event of a default, the holder of the guaranteed portion has the option to request the originating bank to repurchase its portion before presenting the loan to the SBA for ultimate disposition and collection. In addition, some banks may repurchase assets and absorb any loss even when no legal responsibility exists. It is necessary to determine management's practice in order to evaluate the degree of risk involved. If management routinely repurchases assets that were sold without recourse, a contingency liability should be recognized. The amount of the liability should be based on historical data.

Contingent liabilities may also result if the bank, as the seller of a loan without recourse, does not comply with provisions of the agreement. Noncompliance may result from a number of factors, including failure on the part of the selling institution to receive collateral and/or security agreements, obtain required guarantees, or notify the purchasing party of default or adverse financial performance by the borrower. The purchaser of a loan may also assert claims that the financial information, which the purchaser relied on when acquiring the loan, was inaccurate, misleading, or fraudulent and that the selling bank was aware of the deficiencies. Therefore, a certain degree of risk may in fact be evident in assets allegedly sold without recourse. Examiners need to be mindful of this possibility and its possible financial consequences on the bank under examination.

Banks also face credit, liquidity, and interest-rate risk in the period in which they accumulate the assets for sale. Especially in mortgage banking activities, the need to carefully monitor interest-rate risk in the "pipeline" represents one of the significant risks of the business. Sellers of participations also face counterparty risk similar to that of a funding desk, because the loan-sales operation depends on the ongoing willingness of purchasers to roll over existing participations and to buy new ones. In addition, many banks sell loans in the secondary market but retain the responsibility for servicing the loans.

Accounting Issues

For regulatory reporting purposes, some transactions involving the "sale" of assets must be reported as financing transactions (that is, as borrowings secured by the assets "sold"), and others must be reported as sales of the assets involved. The treatment required for any particular transfer of assets depends on whether the "seller" retains risk in connection with the transfer of the assets. In general, to report the transfer of assets as a sale, the selling institution must retain no risk of loss or obligation for payment of principal or interest.

All recourse arrangements should be documented in writing. If a loan is sold with recourse back to the seller, the selling bank has, in effect, retained the full credit risk of the loan, and its lending limit to the borrower is not reduced by the amount sold. Loans sold with recourse are to be treated as borrowings of the selling bank from the purchasing bank. Examiners should consider asset sales subject to formal or informal repurchase agreements (or understandings)

to be sales "with recourse" regardless of other wording in the agreement to the contrary.

In determining the true recourse nature of an asset sale, examiners must determine the extent to which the credit risk has been transferred from the seller to the purchaser. In general, if the risk of loss or obligation for payments of principal or interest is retained by, or may ultimately fall back upon, the seller or lead bank, the transaction must be reported by the seller as a borrowing from the purchaser and by the purchaser as a loan to the seller. Complete details on the treatment of asset sales for purposes of the report of condition and income are found in the glossary of the Instructions for the Preparation of the Report of Condition and Income under the entry "sales of assets."

OTHER OFF-BALANCE-SHEET ACTIVITIES AND CONTINGENT LIABILITIES

Banks often provide a large number of customer services, which normally do not result in transactions subject to entry on the general ledger. These customer services include safekeeping, the rental of safe deposit boxes, the purchase and sale of investments for customers, the sale of traveler's checks, the sale of U.S. Savings Bonds, collection services, federal funds sold as agent, operating leases, and correspondent bank services. It is the bank's responsibility to ensure that collateral and other nonledger items are properly recorded and protected by effective custodial controls. Proper insurance must also be obtained to protect against claims arising from mishandling, negligence, mysterious disappearance, or other unforeseen occurrences. Failure to take these protective steps may lead to contingent liabilities. In addition, pending litigation in which the bank is a defendant could expose the bank to substantial risk of loss. Refer to section 4000, "Other Examination Areas," in this manual for further information.

Banks often enter into operating leases as lessees of buildings and equipment. The arrangements should be governed by a written lease. For a material lease, the examiner must determine whether the lease is truly an operating lease or if it is a capitalized lease pursuant to FASB 13. Capitalized leases and associated obligations must be recorded on the books of the bank in accordance with FASB 13 and the instructions for the preparation of the Report of Condition and Income. Refer to the instructions for the call report and to section 2190, "Bank Premises and Equipment," in this manual for further information about capitalized leases.

While operating leases do not affect the bank's capital ratios, the costs of an operating lease may have a material effect upon the earnings of the bank. Moreover, operating leases may involve other responsibilities for the bank, and the bank's failure to perform these responsibilities may ultimately result in litigation and loss to the bank. The examiner must be cognizant of the requirements imposed on the bank by its leasing arrangements.

Some banks purchase federal funds from smaller correspondent banks as agent. This off-balance-sheet activity is more fully discussed in section 2030, "Bank Dealer Activities," in this manual.

Contingent Claims from Off-Balance-Sheet Credit Activities

Examination Objectives

Effective date November 1995

Section 4110.2

1. To determine if policies, practices, procedures, and internal controls regarding contingent claims from off-balance-sheet credit activities are adequate.
2. To determine if bank officers are operating in conformance with the established guidelines.
3. To evaluate the off-balance-sheet credit activities for credit quality and collectibility.
4. To determine the scope and adequacy of the audit function.
5. To determine compliance with applicable laws and
6. To initiate corrective action when policies, practices, procedures, or internal controls are deficient or when violations of laws or regulations have been noted.

To meet competitive pressures, banks provide a large number of customer services that normally do not result in assets and liabilities subject to entry on the general ledger, but that may involve significant risk. These customer services include fiduciary accounts, investment management, customer safekeeping, rental of safe deposit box facilities, purchase and sale of investments for customers, sale of traveler's checks, and collection department services. The bank is responsible for properly maintaining and safeguarding all consigned items. Banks accomplish the necessary control and review of consigned and collection items through non-ledger control or memorandum accounts. Automated systems, such as a Securities Movements Accounting and Control system (SMAC), can provide proper control for fiduciary, customer safekeeping, custodial, and investment management accounts.

CUSTOMER SAFEKEEPING

Custodial and Investment Management Accounts

Banks may act as custodians for customers' investments such as stocks, bonds, or gold. Custodial responsibilities may involve simple physical storage of the investments, as well as recording sales, purchases, dividends, and interest.[1] On the other hand, responsibilities may be expanded to include actually managing the account. This type of account management includes advising customers when to sell or buy certain investments, as well as meeting their recording requirements. In addition, the bank may lend securities from custodial accounts if authorized by the customer. This transaction allows the bank, as custodian, to charge a fee for lending the securities, thereby reducing its net custody costs. Also, both the bank and the custodial account benefit from interest earned on the transaction. This type of transaction should be governed by a policy that clearly specifies quality and maturity parameters. Additionally, to prevent defaults, borrowers should be subject to minimum credit standards, ongoing financial monitoring, and aggregate borrowing limits. Banks may also indemnify customer accounts against losses from a borrower or collateral default. Such indemnification creates a contingent financial risk to the institution.

Before providing such management and/or lending services, the bank should seek the advice of legal counsel about applicable state and federal laws concerning that type of bank-customer relationship. In addition, the use of signed agreements or contracts that clearly define the services to be performed by the bank is a vitally important first step in limiting the bank's potential liability and risk. The bank must also ensure that a proper control environment, including joint custody and access procedures, is established and maintained in support of custodial and management activities. Clearly, the largest and most active companies take on an increased level of risk. For companies that are aggressively pursuing custodial services or other nontraditional lines of business, the examiner should consider an expanded scope of review for these activities.

Safe Deposit Boxes

When banks maintain safe deposit box facilities, the bank and the customer enter into a contract whereby the bank receives a fee for renting safe deposit boxes. The bank assumes the responsibility of exercising reasonable care and precaution against loss of the box's contents. When a loss does occur, unless the bank can demonstrate it has maintained the required standard of care, it could be held liable for the loss. The required standard of care is defined as that which would be taken by a reasonably prudent and careful person engaged in the same business. Two different keys are required to open the box, and the customer and the bank each have one. Careful verification of a customer's identification is critical to meeting an appropriate standard of care. The customer is not required to disclose the contents of the box to the bank and upon court order the bank may gain access to the box without the presence of the customer.

1. Collection of interest and dividend income cannot be facilitated by the bank where the securities held are still in the customer's name, unless the paying agent is advised to change the dividend/interest address. Typically, when securities remain in the registered name of the holder, the holder continues to receive the dividend/interest payments. If the securities are re-registered into the name of the bank (or its nominee), then dividends and interest are received by the bank for the credit of the custodial customer.

Safekeeping

In addition to items held as collateral for loans, banks occasionally hold customers' valuables for short periods of time. The bank may or may not charge a fee for the service. Although it is a convenience for bank customers, many banks attempt to discourage the practice by emphasizing the benefits of a safe deposit box. When it is not possible or practical to discourage a customer, the same procedures that are employed in handling collateral must be followed. Items to be stored should be inventoried by two persons and maintained under dual control in the bank's vault. A multicopy, prenumbered, safekeeping receipt should be prepared with a detailed description of the items accepted and it should be signed by the customer. Sealed packages with contents unknown to the bank should never be accepted for safekeeping.

COLLECTION ITEMS

The collection department is one of the most diversified areas in the bank. It engages in receiving, collecting, and liquidating items which generally require special handling and for which credit normally is given only after final payment is received. The bank acts as agent for its customers or correspondents and receives a fee for that service. Even though general ledger accounts rarely are used in the collection process, the importance and value of customer assets under bank control demand the use of accounting procedures adequate to provide a step-by-step historical summary of each item processed. An audit trail must be developed to substantiate the proper handling of all items and to reduce the bank's potential liability.

CONSIGNED ITEMS

The most common items held on consignment by banks are unissued gift or traveler's checks; commemorative coins, postage stamps, and other consigned or promotional assets; and gold. Traveler's checks may be useful to customers because of the possibility that customers can obtain a refund if the checks are lost or stolen. Traveler's checks are issued for a fee or commission shared by the consignor and the issuing bank. Generally, a working supply of the checks is maintained at the teller line or selling station and a reserve supply is maintained under dual control in the bank's vault.

Under paragraph 7 of section 5136 of the Revised Statutes, national banks may exercise their powers ''by buying and selling exchange, coin and bullion.'' This statute is applied to state member banks under section 9, paragraph 20, of the Federal Reserve Act. Consequently, banks may deal only in gold or silver that qualifies as coin or bullion. The term ''coin'' means coins minted by a government or exact restrikes, minted at a later date by, or under the authority of, the issuing government.

Rarely does a bank receive sufficient revenues from the above transactions to cover the cost of handling them. However, banks must offer a full range of services to be competitive and attract customers. The bank assumes the responsibility and related contingent liability to properly maintain the assets of others and to properly record all transactions involved with the consigned items.

INTERNAL CONTROL CONSIDERATIONS

It is essential that bank policy provides for proper internal controls, operating procedures, and safeguards. In all cases, control totals must be generated and the function balanced periodically by someone not associated with the function. Proper insurance protection must also be obtained to protect against claims arising from mishandling, negligence, mysterious disappearance, or other unforeseen occurrences. If an employee should, by fraud or negligence, permit unauthorized removal of items held for safekeeping or issue traveler's checks improperly, the bank may be held liable for losses. Therefore, banks should maintain adequate bonding for contingent liabilities and the examiner should review applicable insurance policies.

1. To determine if the policies, practices, procedures, and internal controls regarding custodial activities, consigned items, and other non-ledger control accounts are adequate.
2. To determine if bank officers and employees are operating in conformance with the established guidelines.
3. To determine the scope and adequacy of the audit function.
4. To determine compliance with laws and regulations.
5. To initiate corrective action when policies, practices, procedures, or internal controls are deficient or when violations of laws or regulations have been noted.

1. If selected for implementation, complete or update the Consigned Items and Other Non-Ledger Control Accounts section of the Internal Control Questionnaire.
2. Based on the evaluation of internal controls and the work performed by internal/external auditors, determine the scope of the examination.
3. Test for compliance with policies, practices, procedures and internal controls in conjunction with performing the remaining examination procedures. Obtain a listing of any deficiencies noted in the latest review done by internal/external auditors from the examiner assigned ''Internal Control'' and determine if appropriate corrections have been made.
4. Obtain a listing of consigned items or assets, payment instruments, and other non-ledger control accounts from the bank.
5. Scan any existing control accounts for any significant fluctuations and determine the cause of fluctuations.
6. Compare bank control records to remittance records for unissued U.S. savings bonds and state-issued food stamp value-payment cards or instruments.
7. Determine compliance with laws and regulations pertaining to non-ledger control accounts by determining, through observation and discussion with management, that there exist no violation of the prohibition against a bank participating in lotteries (section 9A of the Federal Reserve Act (12 USC 25A)).
8. Prepare in appropriate report form, and discuss with appropriate officer(s):
   a. Violations of laws and regulations.
   b. Recommended corrective action when policies, practices or procedures are deficient.
9. Update the workpapers with any information that will facilitate future examinations.

Review the bank's internal controls, policies, practices and procedures for consigned items and other non-ledger items. The bank's system should be documented in a complete and concise manner and should include, where appropriate, narrative descriptions, flowcharts, copies of forms used, and other pertinent information. Items marked with an asterisk require substantiation by observation or testing.

SAFE DEPOSIT BOXES

1. Has counsel reviewed and approved the lease contract in use which covers the rental, use and termination of safe deposit boxes?

*2. Is a signed lease contract on file for each safe deposit box in use?

3. Are receipts for keys to the safe deposit box obtained?
4. Are officers or employees of the bank prohibited from acting as a deputy or having the right of access to safe deposit boxes except their own or one rented in the name of a member of their family?
5. Is the guard key to safe deposit boxes maintained under absolute bank control?
6. Does the bank refuse to hold, for renters, any safe deposit box keys?
7. Is each admittance slip signed in the presence of the safe deposit clerk and the time and date of entry noted?
8. Are admittance slips filed numerically?
9. Are vault records noted for joint tenancies and co-rental contracts requiring the presence of two or more persons at each access?
10. Are the safe deposit boxes locked closed when permitting access and the renter's key removed and returned to the customer?
11. Is the safe deposit clerk prohibited from assisting the customer in looking through the contents of a box?
12. Does the safe deposit clerk witness the relocking of the box?
13. Are all coupon booths examined by an attendant after being used but before being assigned to another renter, to be sure the previous person did not leave behind anything of value?
14. Has a standard fee schedule for this service been adopted?
15. Are all collections of rental income recorded when received?
16. Are all safe deposit boxes where lessee is delinquent in rent, flagged or otherwise marked so that access will be withheld until rent is paid?
17. Is there a file maintained of all attachments, notices of bankruptcy, letters of guardianship and letters testamentary served on the bank?
18. Is an acknowledgment of receipt of all property, and a release of liability signed upon termination of occupancy?
19. Are locks changed when boxes are surrendered, whether or not keys are lost?
20. Is drilling of boxes witnessed by two individuals?
21. Are the contents of drilled boxes inventoried, packaged, and placed under dual control?

*22. Are all extra locks and keys maintained under dual control?

Conclusion

23. Is the foregoing information an adequate basis for evaluating internal control in that there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
24. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

ITEMS IN SAFEKEEPING

*25. Are such items segregated from bank-owned assets and maintained under dual control?

26. Is there a set charge or schedule of charges for this service?

27. Do bank policies prohibit holding items in safekeeping free of charge?
28. Are duplicate receipts issued to customers for items deposited in safekeeping?
29. Are the receipts prenumbered?
*30. Is a safekeeping register maintained to show details of all items for each customer?
*31. Is a record maintained of all entries to custodial boxes or vaults?
32. Does the bank refuse to accept sealed packages when the contents are unknown?
33. If the bank has accepted sealed packages for safekeeping, the contents of which are not described, has the approval of the bank's counsel been obtained?
34. When safekeeping items are released, are receipts obtained from the customer?

Conclusion

35. Is the foregoing information an adequate basis for evaluating internal control in that there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
36. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

CUSTODIAN ACCOUNTS

(Omit this section if the bank's trust department handles such accounts).

*37. Does the bank have written contracts on hand for each account that clearly define the functions to be performed by the bank?
38. Has bank counsel reviewed and approved the type and content of the contracts being used?
39. Does the bank give customers duplicate receipts with detailed descriptions, including dates of coupons attached, if applicable, for all items accepted?
40. Are those receipts prenumbered?
41. Do bank procedures prohibit its holding any investments not covered by a sale or purchase order in this department?
42. Are all orders for the purchase and sale of investments properly authorized in the account contract or signed by customers?
43. For coupon securities held by the bank:
    a. Is a tickler file or other similar system used to ensure prompt coupon redemption on accounts where the bank has been authorized to perform that service?
    b. Are procedures in effect to prevent clipping of coupons where bank is not so authorized?
    c. Have procedures been adopted to insure prompt customer credit when coupon proceeds or other payments are received?

*44. Are all investment items handled in this area maintained under dual control?
45. Have procedures been established for withdrawal and transmittal of items to customers?
*46. Does an officer review and approve all withdrawals prior to the transaction?
47. Has a standard fee schedule for this service been adopted?

Conclusion

48. Is the foregoing information an adequate basis for evaluating internal control in that there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
49. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

COLLECTION ITEMS

50. Is access to the collection area controlled (if so, indicate how)?
*51. Are permanent registers kept for incoming and outgoing collection items?
52. Are all collections indexed in the collection register?
53. Do such registers furnish a complete history of the origin and final disposition of each collection item?

54. Are receipts issued to customers for all items received for collection?
55. Are serial numbers or prenumbered forms assigned to each collection item and all related papers?
*56. Are all incoming tracers and inquiries handled by an officer or employee not connected with the processing of collection items?
57. Is a record kept to show the various collection items which have been paid and credited as a part of the day's business?
58. Is an itemized daily summary made of all collection fees, showing collection numbers and amounts?
59. Are employees handling collection items periodically rotated, without advance notification, to other banking duties?
*60. Is the employee handling collection items required to make settlement with the customer on the same business day that payment of the item is received?
61. Does the bank have an established policy of not allowing the customer credit until final payment is received?
*62. Have procedures been established, including supervision by an officer, for sending tracers and inquiries on unpaid collection items in the hands of correspondents?
63. In the event of nonpayment of a collection item, is the customer notified and the item promptly returned?
*64. Are the files of notes entered for collection clearly and distinctly segregated from bank-owned loans and discounts?
*65. Are collection notes above maintained under memorandum control and is the control balanced regularly?
66. Are collection files locked when the employee handling such items is absent?
67. Are vault storage facilities provided for collection items carried over to the next day's business?
*68. Does the collection teller turn over all cash to the paying teller at the close of business each day and start each day with a standard change fund?
69. Has a standard fee schedule for this service been adopted?
70. Is the fee schedule always followed?
71. Is a permanent record maintained for registered mailed?

Conclusion

72. Is the foregoing information an adequate basis for evaluating internal control in that there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
73. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

CONSIGNED ITEMS

*74. Is the reserve stock of consigned items maintained under dual control?
75. Are working supplies kept to a reasonable minimum, i.e., two or three days' supply, and adequately protected during banking hours?
*76. Is a memorandum control maintained of consigned items?
77. Are separate accounts with the consignor maintained at each issuing location (branch), if applicable?
*78. Is the working supply put in the vault at night and over weekends or holidays or is it otherwise protected?
79. Are remittances for sales made on a regularly scheduled basis, if not daily?

Conclusion

80. Is the foregoing information an adequate basis for evaluating internal control in that there are no significant deficiencies in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
81. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

Modern economies require an efficient system for transferring funds between financial institutions and between financial institutions and their customers. Banks and other depository institutions use payment systems both to transfer funds related to their own operations—for example, when engaging in federal-funds transactions—and to transfer funds on behalf of their customers. Depository institutions and the Federal Reserve together provide the basic infrastructure for the nation's payment system.

Commercial banks maintain accounts with each other and with the Federal Reserve Banks; through these accounts, the payments of the general public are recorded and ultimately settled. The demand for electronic funds transfer (EFT) services has increased with improved data communication and computer technology. Community banks that previously executed EFT transactions through a correspondent can now initiate their own same-day settlement transactions nationwide. The need for same-day settlement transactions has precipitated financial institutions' increased reliance on EFT systems. Financial institutions commonly use their EFT operations to make and receive payments, buy and sell securities, and transmit payment instructions to correspondent banks worldwide. In the United States, most of the dollar value of all funds transfers is concentrated in two electronic payment systems: the Fedwire Funds Service, which is a real-time gross settlement system provided by the Federal Reserve Banks, and the Clearing House Interbank Payments System (CHIPS), which is a private-sector multilateral settlement system owned and operated by the Clearing House Payments Company.

Final settlement occurs when payment obligations between payment-system participants are extinguished with unconditional and irrevocable funds. For transactions settled in physical currency, payment and settlement finality occur simultaneously. On occasion, settlement finality may not occur on the same day a payment is made. Without immediate settlement finality, the recipient of a payment faces the uncertainty of not receiving the value of funds that has been promised. The exposure to this uncertainty is generally referred to as *payment system risk* (PSR).

Payment system risk refers to the risk of financial loss to the participants in, and operators of, payment systems due to a variety of exposures, such as counterparty or customer default, operational problems, fraud, or legal uncertainty about the finality of settled payments. A major source of payment system risk arises when participants in, or the operator of, a payment system extends unsecured, intraday credit to facilitate the smooth and efficient flow of payments. For example, the aggregate value of intraday credit extended by the Federal Reserve, in the form of daylight overdrafts in institutions' Federal Reserve accounts, is substantial and creates significant credit exposure for the Federal Reserve Banks.

A daylight overdraft occurs whenever an institution has a negative account balance during the business day. Such a credit exposure can occur in an account that an institution maintains with a Federal Reserve Bank or with a private-sector financial institution. At a Reserve Bank, a daylight overdraft occurs when an institution has insufficient funds in its Federal Reserve account to cover Fedwire funds transfers, incoming book-entry securities transfers, or other payment activity processed by the Reserve Bank, such as automated clearinghouse or check transactions. Similarly, banks are exposed to credit risk when they permit their customers to incur daylight overdrafts in their accounts. More specific information about the types of risks involved under the rubric of payment systems risk is discussed later in this section.

When developing an institution's overview, performing annual and quarterly risk assessments, and conducting the institution's examination, examiners should review an institution's payment system risk and EFT practices. Supervisory and examination guidance and procedures should be followed to determine the risk assessment, matrix, supervisory plan, and scope of an examination. This guidance should also be used when conducting the examination. An overall initial analysis of an institution's payment system risk practices can provide examiners with quick insight on the adequacy of its current internal controls and risk-management practices, and on whether the institution's payment activity creates intraday exposures that may pose significant risk if not managed properly.

In general, examiners should review the frequency, magnitude, and trend of daylight overdrafts in an institution's Federal Reserve account, as well as any breaches of its net debit cap.

Examiners should analyze the reasons for the daylight overdrafts and cap breaches; the nature of the transactions causing the overdrafts (for example, correspondent check clearings or funds transfers); whether the number of customers, correspondents, and respondents is concentrated among only a few entities; whether there is a clear pattern of transactions; and the types of activities involved. In addition, examiners should review and determine the adequacy of the resolution by the board of directors authorizing the institution's net debit cap and use of Federal Reserve intraday credit (as required by the PSR policy). The examiners' most important goal is to ensure that banks have and use appropriate risk-management policies and procedures that effectively monitor and control their exposure to payment system risk.

TYPES OF PAYMENT SYSTEMS

An understanding of the mechanics of the various payment systems is necessary to evaluate the operational procedures depository institutions use to control payment-processing risks for their own or their customers' accounts.

Funds Transfer Systems

Fedwire Funds Service

The Fedwire funds-transfer system is a real-time gross settlement system in which depository institutions initiate funds transfers that are immediate, final, and irrevocable when processed. Depository institutions that maintain a master account with a Federal Reserve Bank may use Fedwire to directly send or receive payments to, or receive payments from, other account holders directly. Depository institutions use Fedwire to handle large-value and time-critical payments, such as payments for the settlement of interbank purchases and sales of federal funds; the purchase, sale, and financing of securities transactions; the disbursement or repayment of loans; and the settlement of real estate transactions.

In the Fedwire funds-transfer system, only the originating financial institution can remove funds from its Federal Reserve account. Originators provide payment instructions to the Federal Reserve either online or offline. Online participants send instructions through a mainframe or PC connection to Fedwire, and no manual processing by the Federal Reserve Banks is necessary. Offline participants give instructions to the Reserve Banks by telephone. Once the telephone request is authenticated, the Reserve Bank enters the transfer instruction into the Fedwire system for execution. The manual processing required for offline requests makes them more costly; thus, they are suitable only for institutions that have small, infrequent transfers. (For further information, see www.federalreserve.gov/paymentsystems/)

CHIPS

The Clearing House Interbank Payments System (CHIPS) is a large-value funds-transfer system for U.S. dollar payments between domestic or foreign banks that have offices located in the United States. CHIPS provides a final intraday settlement system, continuously matching, netting, and settling queued payment orders throughout the business day.

All CHIPS payment orders are settled against positive balances and are simultaneously offset by incoming payment orders, or some combination of both. To facilitate this process, the funding participants jointly maintain an account (CHIPS account) on the books of the Federal Reserve Bank of New York. Each CHIPS participant must fund this account via a Fedwire funds transfer to fulfill its pre-funded opening-position requirement. These required balances are then used to settle payment orders throughout the day.

During the operating day, participants submit payment orders to a centralized queue maintained by CHIPS. Payment orders that do not pass certain settlement conditions are held in the central queue until an opportunity for settlement occurs or until the end-of-day settlement process. The sending and receiving participants are not obligated to settle these queued payment orders.

Each afternoon, each participant with a closing-position requirement must transfer, through Fedwire, its requirement to the CHIPS account at the Federal Reserve Bank of New York.[1] These requirements, when delivered, are credited to participants' balances at CHIPS.

1. Although CHIPS no longer makes distinctions between settling and nonsettling participants, CHIPS participants can use nostro banks to make transfers on their behalf.

After completion of this process, CHIPS will transfer to those participants who have any balances remaining, that is, participants in an overall net positive position for the day, the full amount of those positions. (For further information, see the CHIPS rules at www.chips.org.)

Manual Systems

Not all financial institutions employ an EFT system. Some banks execute such a small number of EFT transactions that the cost of a computer-based system such as Fedwire is prohibitive. Instead, these banks will continue to execute EFTs by a telephone call to a correspondent bank. Executing EFT transactions in this way is an acceptable practice as long as the bank has adequate internal control procedures.

Message Systems

The message systems employed by financial institutions, corporations, or other organizations to originate payment orders—either for their own benefit or for payment to a third party—are indispensable components of funds-transfer activities. Unlike payment systems, which transmit actual debit and credit entries, message systems process administrative messages and instructions to move funds. The actual movement of the funds is then accomplished by initiating the actual entries to debit the originating customer's account and to credit the beneficiary's account at one or more financial institutions. If the beneficiary's account or the beneficiary bank's account is also with the originator's bank, the transaction is normally handled internally through *book entry.* If the beneficiary-related accounts are outside the originating customer's bank, the transfer may be completed by use of a payment system such as Fedwire or CHIPS. The means of arranging payment orders ranges from manual methods (for example, memos, letters, telephone calls, fax messages, or standing instructions) to electronic methods using telecommunications networks. These networks may include those operated by the private sector, such as SWIFT or Telex, or other networks operated internally by particular financial institutions.

Even though the transfers initiated through systems such as SWIFT and Telex do not result in the immediate transfer of funds from the issuing bank, they do result in the issuing bank's having an immediate liability, which is payable to the disbursing bank. Therefore, the internal operating controls of these systems should be as stringent as the ones implemented for systems such as Fedwire and CHIPS.

SWIFT

The Society for Worldwide Interbank Financial Telecommunications (SWIFT) is a nonprofit cooperative of member banks that serves as a worldwide interbank telecommunications network for structured financial messaging. Based in Brussels, Belgium, SWIFT is the primary system employed by financial institutions worldwide to transmit either domestic or international payment instructions. (For further information, see www.swift.com.)

TELEX

Several private telecommunications companies offer worldwide or interconnected services that provide a printed permanent record of each message transmitted. Telex is the primary message system for institutions that do not have access to SWIFT. The Telex systems do not include built-in security features. Telex users exchange security codes, and senders sequentially number messages sent to another institution.

Automated Clearinghouse and Check Transactions

The automated clearinghouse (ACH) is an electronic payment delivery system used to process low-dollar retail payments. The system is used for preauthorized recurring payments and one-time payments. First introduced in the early 1970s as a more efficient alternative to checks, ACH has evolved into a nationwide mechanism that processes electronically originated credit and debit transfers for any participating institution nationwide. An alternative to paper checks, the ACH handles billions of payments annually.

Financial institutions are encouraged to obtain a copy of the ACH rules of the National Automated Clearing House Association (NACHA): *A*

Complete Guide to Rules and Regulations Governing the ACH Network. The ACH rules provide detailed information on rule changes, their operational impact, and whether any software changes are required. The rulebook is designed to help financial institutions comply with the current NACHA rules, which are applicable to all ACH participants and include a system of national fines. (For further information, see www.nacha.org.)

The Federal Reserve ACH is governed by Operating Circular #4, "Automated Clearing House Items." Other important federal legislation concerning the ACH can be found in Regulation E (primarily regarding consumer rights pertaining to electronic funds transfers) and Regulation CC (concerning the availability of funds). (For further information, see www.frbservices.org.)

There are two types of ACH transactions: ACH debits and ACH credits. In an ACH debit transaction, the originator of the transaction is debiting the receiver's account. Therefore, funds flow from the receiver to the originator of the transaction. Mortgage payments for which consumers authorize the mortgage company to debit their accounts each month are examples of ACH debit transactions. ACH debits are also being used increasingly for one-time payments authorized through the telephone, Internet, or mail.

ACH debit transactions have similarities to check transactions. Both receivers of ACH debit files and payers of checks have the right to return transactions for various reasons, such as insufficient funds in the account or a closed account. The major risk facing institutions that originate ACH debit transactions and collect checks for customers is return-item risk. Return-item risk extends from the day funds are made available to the customer until the individual return items are received.

In an ACH credit transaction, the originator of the transaction is crediting the receiver's account. An ACH credit transaction is similar to Fedwire funds transfers in that funds flow from the originator of the transaction to the receiver. A company payroll payment to its employee would be an example of an ACH credit transaction: the bank sending payments on behalf of a customer (the employer in this instance) has a binding commitment to settle for the payments when the bank sends them to the ACH operator. Since the ACH is a value-dated mechanism, that is, transactions may be originated one or two days before the specified settlement day, the bank is exposed to temporal credit risk that may extend from one to three business days, depending on when the customer (the employer) funds the payments it originates. If the customer fails to fund the payments on the settlement day, the potential loss faced by the originating bank is equal to the total value of payments from the time the payments are sent to the ACH operator until the customer funds these payments.

SECURITIES CLEARING AND SETTLEMENT SYSTEMS

Fedwire Securities

The Fedwire Securities Service is a securities settlement system that provides safekeeping services and transfer and settlement services. The safekeeping services enable eligible participants to hold securities issued by the U.S. Department of the Treasury, federal agencies, government-sponsored enterprises (GSEs), and certain international organizations in securities accounts at the Reserve Banks. The transfer and settlement services enable eligible participants to transfer securities to other eligible participants against payment or free of payment.

Participants in the Fedwire Securities Service generally maintain a master account and have routine access to Reserve Bank intraday credit. Like the Fedwire Funds Service, access to the Fedwire Securities Service is limited to depository institutions and a few other organizations, such as federal agencies, state government treasurers' offices (which are designated by the U.S. Department of the Treasury to hold securities accounts), and limited-purpose trust companies that are members of the Federal Reserve System. Nonbank brokers and dealers typically hold and transfer their securities through clearing banks, which are Fedwire participants that provide specialized government securities clearing services. (For more information, see www.federalreserve.gov/paymentsystems/)

Securities transfers can be made free of payment or against a designated payment. Most securities transfers involve the delivery of securities and the simultaneous exchange of payment for the securities, a transaction called delivery-versus-payment. The transfer of securities and related funds (if any) is final at the time of transfer.

Transfer-Size Limit on Book-Entry Securities

Secondary-market book-entry securities transfers on Fedwire are limited to a transfer size of $50 million par value. This limit is intended to encourage partial deliveries of large trades in order to reduce position building by dealers, a major cause of book-entry securities overdrafts before the introduction of the transfer-size limit and daylight-overdraft fees. This limitation does not apply to—

- original-issue deliveries of book-entry securities from a Reserve Bank to an institution, or
- transactions sent to or by a Reserve Bank in its capacity as fiscal agent of the United States, government agencies, or international organizations.

Thus, requests to strip or reconstitute Treasury securities or to convert bearer or registered securities to or from book-entry form are exempt from this limitation. Also exempt are pledges of securities to a Reserve Bank as principal (for example, discount window collateral) or as agent (for example, Treasury Tax and Loan collateral).

Private Systems

In addition to U.S. Treasury and government-agency securities, major categories of financial instruments commonly traded in the United States include corporate equities and bonds, municipal (state and local) government securities, money market instruments, and derivatives such as swaps and exchange-traded options and futures. These instruments are generally traded through recognized exchanges or over-the-counter dealer markets. The mechanisms for clearance and settlement vary by type of instrument and generally involve specialized financial intermediaries, such as clearing corporations and depositories. Clearing corporations provide trade comparison and multilateral netting of trade obligations. Securities depositories, in contrast, hold physical securities and provide book-entry transfer and settlement services for their members.

The vast majority of corporate equity and bond trades are cleared through the National Securities Clearing Corporation (NSCC). Most corporate securities, as well as municipal government bonds, are held at the Depository Trust Company (DTC) in New York. Settlement of securities cleared through the NSCC is effected by book-entry transfers at the DTC. The DTC and the NSCC are owned by the Depository Trust and Clearing Corporation, an industry-owned holding company. (For more information, see www.dtcc.com.)

U.S. Treasury, federal-agency, and mortgage-backed securities are generally traded in over-the-counter markets. The Fixed Income Clearing Corporation (FICC) compares and nets its members' trades in most U.S. Treasury and federal-agency securities. The FICC relies on the Fedwire securities service, discussed above, to effect final delivery of securities to its participants. The FICC is owned by the DTCC. (For more information see www.dtcc.com.)

The FICC also provides automated post-trade comparison, netting, risk-management, and pool-notification services to the mortgage-backed securities market. The FICC provides its specialized services to major market participants active in various Government National Mortgage Association (GNMA), Federal Home Loan Mortgage Corporation (Freddie Mac or FHLMC), and Federal National Mortgage Association (Fannie Mae or FNMA) mortgage-backed securities programs. The net settlement obligations of FICC participants are settled through the Fedwire book-entry securities system.

POLICY ON PAYMENT SYSTEM RISK

The Federal Reserve's Policy on Payment System Risk (the PSR policy) addresses in part, the risks that payment and securities settlement systems present to the Federal Reserve Banks, the banking system, and other sectors of the economy. Part II of the PSR policy focuses on institutions'[2] use of Federal Reserve intraday credit.[3] An integral component of the PSR

2. The PSR policy uses the term *institutions*, which refers to depository institutions, U.S. branches and agencies of foreign banking organizations, Edge and agreement corporations, bankers' banks, limited-purpose trust companies, government-sponsored enterprises, and international organizations, unless the context indicates a different meaning.

3. Part I of the PSR policy addresses risks in private-sector payment systems and settlement. The full text of the PSR policy is available at www.federalreserve.gov/paymentsystems/psr_policy.htm.

policy is a program to control the risks in the payment system, including institutions' use of Federal Reserve intraday credit, commonly referred to as *daylight credit* or *daylight overdrafts*. Individual Reserve Banks are responsible for administering the Board's PSR policy and ensuring compliance by institutions. A primary objective of examiners when evaluating payment system risk is to ensure that banks using Federal Reserve payment services comply with the Board's PSR policy.

PSR Policy Objectives

Like institutions that offer payment services to customers, Federal Reserve Banks encounter credit risk when they process payments for institutions that hold accounts with them. The Federal Reserve guarantees settlement on Fedwire funds and book-entry securities transfers, net settlement service (NSS) entries,[4] and ACH credit originations made by account holders. If an institution were to fail after sending a transaction that placed its account in an overdraft position, the Federal Reserve would be obligated to cover the payment and bear any resulting losses. Risk is present even when an institution overdraws its account at a Reserve Bank for only a few minutes during the day.

Similar types of risk are generated when customers of private financial institutions and participants in some private-sector payment arrangements incur daylight overdrafts. In addition, daylight credit may be a source of systemic risk in the payment system. *Systemic risk* refers to the potential that the failure of one participant in a payment system, or in the financial markets generally, to meet its required obligations will cause other participants or financial institutions to be unable to meet their settlement obligations when due.

The PSR policy allows Reserve Banks to mitigate their credit risk in several ways. For instance, institutions that access daylight credit must satisfy safety-and-soundness requirements. In addition, the policy permits Reserve Banks to protect themselves from risk exposure of individual institutions through such measures as restricting account activity or imposing collateral requirements.

The PSR policy establishes limits on the maximum amount of Federal Reserve daylight credit that an institution may use during a single day or over a two-week period. These limits are sufficiently flexible to reflect the overall financial condition and operational capacity of each institution using Federal Reserve payment services. The policy also permits Reserve Banks to protect themselves from the risk of loss through measures such as reducing net debit caps; imposing collateralization or clearing-balance requirements; and rejecting certain transactions during the day until balances are available in its Federal Reserve account; or, in extreme cases, taking the institution offline or prohibiting it from using Fedwire.

FEDERAL RESERVE INTRADAY CREDIT POLICIES (PART II)

In December 2008, the Board adopted major revisions to part II of the PSR policy that are designed to improve intraday liquidity management and payment flows for the banking system, while also helping to mitigate the credit exposures of the Federal Reserve Banks.[5] The changes included an approach that explicitly recognizes the role of the central bank in providing intraday balances and credit to healthy depository institutions. In addition, the Board revised other elements of the PSR policy dealing with daylight overdrafts, which included adjusting net debit caps, voluntary collateralization of intraday credit, a limit on total daylight overdrafts in institutions' Federal Reserve accounts, and eliminating the current deductible for daylight overdraft fees.

The Board also approved for certain foreign banking organizations a policy change related to the calculation of the deductible amount from daylight overdraft fees and early implementation of the streamlined procedure for maximum daylight overdraft capacity (max cap). The policy changes and the early implementation of the streamlined max cap became effective on March 26, 2009.

Daylight-Overdraft Capacity

Under the Federal Reserve's PSR policy, each

4. The Federal Reserve's NSS provides settlement services to various clearinghouses.

5. See Board's press release at www.federalreserve.gov/newsevents/press/other/20081219a.htm.

Table 1—Net debit cap multiples

	Net debit cap multiples	
Cap categories	*Single-day*	*Two-week average*
High	2.25	1.50
Above average	1.875	1.125
Average	1.125	0.75
De minimis	0.40	0.40
Exempt-from-filing*	$10 million or 0.20	$10 million or 0.20
Zero	0	0

* The net debit cap for the exempt-from-filing category is equal to the lesser of $10 million or 0.20 multiplied by the institution's capital measure.

institution that maintains an account at a Federal Reserve Bank is assigned or may establish a net debit cap, as outlined below. The net debit cap limits the amount of intraday Federal Reserve credit that the institution may use during a given interval. The policy allows financially healthy institutions that have regular access to the discount window to incur daylight overdrafts in their Federal Reserve accounts up to their individual net debit caps. In addition, the policy allows certain institutions to pledge collateral to the Federal Reserve to access additional daylight-overdraft capacity above their net debit caps. In these instances, the institution can incur daylight overdrafts equaling the lesser of its net debit cap and pledged collateral or max cap if it is fully collateralized.

NET DEBIT CAPS

An institution's net debit cap refers to the maximum dollar amount of uncollateralized daylight overdrafts that the institution may incur in its Federal Reserve account. An institution's cap category and its capital measure determine the dollar amount of its net debit cap.[6] An institution's net debit cap is calculated as its cap multiple, as listed in table 1, times its capital measure:

$$\text{net debit cap} = \text{cap multiple} \times \text{capital measure}$$

Because a net debit cap is a function of an institution's capital measure, the dollar amount of the cap will vary over time as the institution's capital measure changes. Unless circumstances warrant a revision, an institution's cap category, however, is normally fixed over a one-year period. Cap categories and their associated cap levels, set as multiples of capital, are listed in table 1.

An institution is expected to avoid incurring daylight overdrafts whose daily maximum level, averaged over a two-week period, would exceed its two-week average cap, and, on any day, would exceed its single-day cap. The two-week average cap provides flexibility, recognizing that fluctuations in payments can occur from day to day. The purpose of the single-day cap is to limit excessive daylight overdrafts on any day and to ensure that institutions develop internal controls that focus on the exposures each day, as well as over time. Institutions in the zero, exempt-from-filing, and de minimis cap categories have one cap that applies to both the single-day peak overdraft and the average overdraft for a two-week period.

The Board's policy on net debit caps is based on a specific set of guidelines and some degree of examiner oversight. Under the Board's policy, a Reserve Bank may limit or prohibit an institution's use of Federal Reserve intraday

6. The capital measure used in calculating an institution's net debit cap depends on its home-country supervisor and chartering authority. For institutions chartered in the United States, net debit caps are multiples of "qualifying" or similar capital measures, that is, those capital instruments that can be used to satisfy risk-based capital standards, as set forth in the capital adequacy guidelines of the federal financial institution regulatory agencies.

credit if (1) the institution's use of daylight credit is deemed by the institution's supervisor to be unsafe or unsound, (2) the institution does not qualify for a positive net debit cap (see section II.C.2., "Cap Categories," of the PSR policy), or (3) the institution poses excessive risk to a Reserve Bank by incurring chronic overdrafts in excess of what the Reserve Bank determines is prudent.

Cap Categories

The PSR policy defines six cap categories: high, above average, average, de minimis, exempt-from-filing, and zero. The high, above-average, and average cap categories are referred to as "self-assessed" caps.

Self-Assessed

To establish a net debit cap category of high, above-average, or average, an institution must perform a self-assessment of its creditworthiness, intraday funds management and control, customer credit policies and controls, and operating controls and contingency procedures. The assessment of creditworthiness is based on the institution's supervisory rating and prompt-corrective-action designation. An institution may be required to perform a full assessment of its creditworthiness in certain limited circumstances, for example, if its condition has changed significantly since the last examination. An institution performing a self-assessment must also evaluate its intraday funds-management procedures and its procedures for evaluating the financial condition of, and establishing intraday credit limits for, its customers. Finally, the institution must evaluate its operating controls and contingency procedures to determine if they are sufficient to prevent losses due to fraud or system failures.

An examiner's review of an institution's assessment is an important part of determining the institution's compliance with the PSR policy. An examiner is responsible for ensuring that the institution has applied the guidelines appropriately and diligently, that the underlying analysis and methodology were reasonable, and that the resulting self-assessment was generally consistent with examination findings. The following discussion is a simplified explanation of the self-assessment factors. A more detailed explanation of the self-assessment process is provided in the *Guide to the Federal Reserve's Payment System Risk Policy.* (The guide is available on the Internet at www.federalreserve.gov/paymentsystems/psr_relpolicies.htm.)

Creditworthiness. Of the four self-assessment factors, creditworthiness is the most influential in determining an overall net debit cap for a given institution. The creditworthiness factor is principally determined by a combination of the institution's capital adequacy and most recent supervisory rating. In the self-assessment, an institution's creditworthiness is assigned one of the following ratings: excellent, very good, adequate, or below standard. An excellent or a very good rating indicates that an institution demonstrates a sustained level of financial performance above its peer-group norm. As a general matter, fundamentally sound institutions that experience only modest weaknesses receive a rating of very good.

Most institutions will use the creditworthiness matrix to determine this component's rating. If an institution's creditworthiness rating is adequate or better, it then proceeds to rate the other three factors in the self-assessment process. The institution's assessment of the other three factors determines whether its composite rating will be lower than or equal to that determined by the creditworthiness factor. If the overall creditworthiness is below standard, then the institution does not qualify for a positive daylight-overdraft cap. In certain limited circumstances, an institution may conduct a full analysis of this component. The matrix and information regarding the full analysis are available in the *Guide to the Federal Reserve's Payment System Risk Policy.*

Intraday funds management and control. The purpose of analyzing intraday funds management and control is to assess an institution's ability to fund its daily settlement obligations across all payment systems in which it participates. The analysis requires a review of funds management, credit, operations personnel, and payment activity over a period of time.

To obtain an accurate understanding of funds movements, an institution must fully understand its daily use of intraday credit as well as its use of intraday credit on average over two-week periods. The analysis should cover a sufficient period of time so that an institution can determine its peak demand for intraday credit and establish its average use of such credit. The

more volatile an institution's payments activity, the longer the interval that is selected for analysis. The analysis incorporates all operational areas with access to payment systems. In addition to large-dollar funds and book-entry securities-transfer activity, the review should address check clearing, ACH, currency operations, and other payment activity that results in relatively large-value settlement obligations. Thus, the analysis should not be limited to online payment systems or to payment systems to which the institution has online access. Additionally, institutions with direct access to Fedwire or to other payment systems in more than one Federal Reserve District must combine all of these access points into a single integrated analysis.

In performing the analysis, the institution considers both liquidity demands and the potential credit risks associated with participation in each payment system. The institution's capacity to settle its obligations in both routine and nonroutine circumstances must be carefully assessed. In many cases, a complete assessment of an institution's ability to control its intraday obligations extends beyond its ability to control its use of Federal Reserve intraday credit within the constraints of its net debit cap. Rather, the assessment extends to the institution's ability to control its position across all payment systems to a level that permits it to fund its obligations regularly. This type of assurance requires an institution to fully understand the nature of its obligations and to establish systems that permit it to monitor daily activity and respond to unusual circumstances.

Customer credit policies and controls. The assessment of an institution's customer credit policies and controls requires two distinct analyses:

- an analysis of the institution's policies and procedures for assessing the creditworthiness of its customers, counterparties, and correspondents and
- an analysis of the institution's ability to monitor the positions of individual customers and to control the amount of intraday and interday credit extended to each customer.

The analyses require the involvement of both credit and operations personnel, and both analyses should focus on the creditworthiness of all customers, including corporate and other institutions that are active users of payment services. In addition, the creditworthiness of correspondents and all counterparties on privately operated clearing and settlement systems must be assessed.

Operating controls and contingency procedures. The purpose of the analysis of operating controls and contingency procedures is to assess the integrity and the reliability of an institution's payment operations to ensure that they are not a source of operating risk. The integrity of operations is of particular concern because operational errors and fraud can increase the cost of payment services and undermine public confidence in the payments mechanism. Similar results can occur if payment systems are unreliable and if parties making and receiving payments do not have confidence that timely payments will be made.

Overall assessment rating. Once the four self-assessment components are analyzed and an overall rating is determined, the institution's self-assessment and recommended cap category must be reviewed and approved by the institution's board of directors at least once each 12-month period. A cap determination may be reviewed and approved by the board of directors of a holding company parent of an institution, provided that (1) the self-assessment is performed by each entity incurring daylight overdrafts, (2) the entity's cap is based on the measure of the entity's own capital, and (3) each entity maintains for its primary supervisor's review its own file with supporting documents for its self-assessment and a record of the parent's board-of-directors review. The directors' approval must be communicated to the Reserve Bank by submission of a board-of-directors resolution. The Reserve Bank then reviews the cap resolution for appropriateness, in conjunction with the institution's primary regulator. If the Reserve Bank determines that the cap resolution is not appropriate, the institution is informed that it must re-evaluate its self-assessment and submit another resolution. A resolution to establish a different cap category may be submitted by the institution, or it may be required by the Reserve Bank before the annual renewal date, if circumstances warrant such a change.

De Minimis

Institutions that qualify for a de minimis net debit cap incur relatively small daylight overdrafts and thus pose little risk to the Federal Reserve. To ease the burden of performing a self-assessment for these institutions, the PSR policy allows institutions that meet reasonable safety-and-soundness standards to incur de minimus amounts of daylight overdrafts without performing a self-assessment. Such an institution may incur daylight overdrafts of up to 40 percent of their capital measure if it submits a board-of-directors resolution.

An institution with a de minimis cap must submit to its Reserve Bank at least once in each 12-month period a copy of its board-of-directors resolution (or a resolution by its holding company's board) approving the institution's use of daylight credit up to the de minimis level. If an institution with a de minimis cap exceeds its cap during a two-week reserve-maintenance period, its Reserve Bank will decide whether the de minimis cap should be maintained or whether the institution will be required to perform a self-assessment for a higher cap.

Exempt-from-Filing

The majority of institutions that hold Federal Reserve accounts have an exempt-from-filing net debit cap. Granted at the discretion of the Reserve Bank, the exempt-from-filing cap category permits institutions that use small amounts of Federal Reserve daylight credit to incur daylight overdrafts that exceed the lesser of $10 million or 20 percent of their capital measure. The Reserve Banks will review the status of an exempt institution that incurs overdrafts in its Federal Reserve account in excess of $10 million or 20 percent of its capital measure on more than two days in any two consecutive two-week reserve-maintenance periods. The Reserve Bank will decide if the exemption should be maintained or if the institution will be required to file for a higher cap. Granting of the exempt-from-filing net debit cap is at the discretion of the Reserve Bank.

Zero

Some financially healthy institutions that could obtain positive net debit caps choose to have zero caps. Often these institutions have very conservative internal policies regarding the use of Federal Reserve daylight credit, or they simply do not want to incur daylight overdrafts and any associated daylight-overdraft fees. If an institution that has adopted a zero cap incurs a daylight overdraft, the Reserve Bank counsels the institution and may monitor the institution's activity in real time and reject or delay certain transactions that would cause an overdraft. If the institution qualifies for a positive cap, the Reserve Bank may suggest that the institution adopt an exempt-from-filing cap or file for a higher cap, if the institution believes that it will continue to incur daylight overdrafts. In addition, a Reserve Bank may assign an institution a zero net debit cap. Institutions that may pose special risks to the Reserve Banks, such as those institutions without regular access to the discount window, those incurring daylight overdrafts in violation of this policy, or those in weak financial condition, are generally assigned a zero cap. New account holders may also be assigned a zero net debit cap.

Maximum Daylight Overdraft Capacity (Max Cap)

While net debit caps provide sufficient liquidity to most institutions, some institutions may experience liquidity pressures. Consequently, certain institutions with self-assessed net debit caps may pledge collateral to their administrative Reserve Bank (ARB) to secure daylight-overdraft capacity in excess of their net debit caps, subject to Reserve Bank approval. This policy is intended to provide extra liquidity through the pledge of collateral to the few institutions that might otherwise be constrained from participating in risk-reducing payment system initiatives. Institutions that request daylight-overdraft capacity beyond the net debit cap must have already explored other alternatives to address their increased liquidity needs.[7] An institution that wishes to expand its daylight-overdraft capacity by pledging collateral should consult with its ARB.[8] The ARB will work with

7. Some potential alternatives available to a depository institution to address increased intraday credit needs include (1) shifting funding patterns, (2) delaying the origination of funds transfers in a way that does not significantly increase operational risks, or (3) transferring some payments-processing business to a correspondent bank.

8. The ARB is responsible for the administration of Federal Reserve credit, reserves, and risk-management policies for a given institution or other legal entity.

an institution that requests additional daylight-overdraft capacity to decide on the appropriate max cap level. When considering the institution's request, the Reserve Bank will evaluate the institution's rationale for requesting additional daylight-overdraft capacity as well as its financial and supervisory information. The financial and supervisory information considered may include, but is not limited to, capital and liquidity ratios, the composition of balance-sheet assets, CAMELS or other supervisory ratings and assessments, and SOSA rankings (for U.S. branches and agencies of foreign banks).[9] Institutions are also expected to submit the following information when requesting a max cap level under general procedures:

- the amount of maximum daylight-overdraft capacity requested
- written justification for requesting additional daylight-overdraft capacity
- written approval from the institution's board of directors or, in the case of U.S. branches and agencies of foreign banks, written approval from the bank's most senior officer responsible for formulating policy at the foreign bank's U.S. head office
- a principal contact at the institution

When deciding whether an institution is eligible for collateralized capacity, the ARB will consider the institution's reasons for applying for additional collateralized capacity; the information related to the institution's condition; and other information, as applicable. If the ARB approves the request for a max cap level, the institution must submit a board-of-directors resolution for the max cap level at least once in each 12-month period, indicating its board-of-directors approval of that level. An institution's max cap is defined as follows:

maximum daylight-overdraft capacity
or max cap =
single-day net debit cap +
collateralized capacity[10]

Institutions with exempt-from-filing and de minimis net debit caps may not obtain additional daylight-overdraft capacity by pledging collateral. These institutions must first obtain a self-assessed net debit cap. Institutions with zero net debit caps also may not obtain additional daylight-overdraft capacity by pledging collateral. If an institution has adopted a zero cap voluntarily, but qualifies for a positive cap, it may not obtain additional daylight-overdraft capacity by pledging collateral without first obtaining a self-assessed net debit cap. Institutions that have been assigned a zero net debit cap by their ARB are not eligible for additional daylight-overdraft capacity.

ROLE OF DIRECTORS

The directors of an institution establish and implement policies to ensure that its management follows safe and sound operating practices, complies with applicable banking laws, and prudently manages financial risks. Given these responsibilities, the directors play a vital role in the Federal Reserve's efforts to reduce risks within the payment system. As part of the PSR policy, the Federal Reserve requests that directors, at a minimum, undertake the following responsibilities:

- Understand the institution's practices and controls for the risks it assumes when processing large-dollar transactions for both its own account and the accounts of its customers or respondents.
- Establish prudent limits on the daylight overdrafts that the institution incurs in its Federal Reserve account and on its privately operated clearing and settlement systems.
- Periodically review the frequency and dollar levels of daylight overdrafts to ensure that the institution operates within the guidelines established by its board of directors. Directors should be aware that, under the Federal Reserve's PSR policy, repeated policy violations could lead to reductions in the institution's daylight-overdraft capacity, or to the imposition of restrictions on its Federal Reserve account activity, either of which could affect the institution's operations.

9. See the full text of the PSR policy to view the streamlined procedures a qualified foreign banking organization may request from its Reserve Bank to obtain a max cap.

10. Collateralized capacity represents the collateralized component of the max cap approved by the Reserve Bank. The amount of collateralized capacity cannot exceed the difference between the institution's max cap level and its net debit cap. For example, if an institution's single-day net debit cap increases as a result of an increase in capital at the institution, its max cap is unchanged, so its collateralized capacity is reduced. The institution's overdraft position will be measured against the lesser of (1) its max cap or (2) its net debit cap plus the amount of collateral pledged.

Each institution that performs a self-assessment for a net debit cap should establish daylight-overdraft policies and controls after considering its creditworthiness, intraday funds management and control, customer credit policies and controls, and operating controls and contingency procedures.

The directors may appoint a committee of directors to focus on the institution's participation in payment systems and its use of daylight credit. Furthermore, a higher-level board of the same corporate family may conduct a self-assessment review, if necessary, and approve a resolution. The board of directors should be aware that delegating the review process to a committee or higher-level board does not absolve the directors from the responsibilities stated in the Federal Reserve's PSR policy. The directors cannot delegate this responsibility to an outside consultant or third-party service provider.

For institutions requesting max caps, the board of directors must understand the use and purposes of the pledged collateral under the PSR policy. The directors must understand the reasons that the institution is applying for additional daylight-overdraft capacity, the amount of the collateralized capacity, and the total amount of the net debit cap plus collateralized capacity.

The Federal Reserve recognizes that directors of foreign banks do not necessarily serve in the same capacity as directors of banks in the United States. Therefore, individuals who are responsible for formulating policy at the foreign bank's head office may substitute for directors in performing the responsibilities specified in the PSR policy.

Cap Resolutions

A board-of-directors resolution is required to establish a cap in the de minimis or self-assessed cap categories (high, above average, or average). In addition, a separate resolution is required for self-assessed institutions that wish to obtain collateralized capacity above their net debit caps (max cap). These resolutions must follow a prescribed format. Specifically, resolutions must include (1) the official name of the institution, (2) the city and state in which the institution is located, (3) the date the board acted, (4) the cap category adopted, (5) the appropriate official signature, and (6) the ABA routing number of the institution. For a board resolution approving the results of a self-assessment, the resolution must identify the ratings assigned to each of the four components of the assessment as well as the overall rating used to determine the actual net debit cap. In addition, the institution should indicate if it did not use the creditworthiness-matrix approach in determining its creditworthiness rating.

An institution's primary supervisor may review resolutions, and any information and materials the institution's directors used to fulfill their responsibilities under the PSR policy. They must be made available to the bank supervisor's examiners. Supporting documentation used in determining an appropriate cap category must be maintained at the institution. At a minimum, the following items must be maintained in the institution's "cap resolution file":

- an executed copy of the resolution adopting the net debit cap and/or max cap;
- worksheets and supporting analysis used in its self-assessment of its own cap category;
- for institutions with self-assessed caps, copies of management's self-assessment of creditworthiness, intraday funds management and control, customer credit policies and controls, and operating controls and contingency procedures;
- minutes and other documentation that serve as a formal record of any directors' discussions on the self-assessment and/or request for max cap;
- status reports the board of directors received on the institution's compliance with both the resolutions adopted by the directors and the PSR policy; and
- other materials that provide insight into the directors' involvement in carrying out their responsibilities under the PSR policy, including special studies or presentations made to the directors.

The board-of-directors resolution for de minimis and self-assessed institutions and for collateralized-capacity resolutions is valid for one year after the Reserve Bank approves the net debit cap or the amount of maximum daylight-overdraft capacity. An institution with a de minimis cap must renew its cap resolution annually by submitting a new resolution to its Reserve Bank. An institution with a self-assessed cap must perform a new self-assessment annually and submit an updated cap resolution to its Reserve Bank. An institution that has a

self-assessed cap and has obtained a max cap must submit a board-of-directors resolution to its Reserve Bank annually. Procedures for submitting these resolutions are the same as those for establishing the initial cap; however, an institution may submit a resolution for a different cap category or a different amount of collateralized capacity, if appropriate. The Reserve Bank, in conjunction with an institution's primary supervisor, will review the appropriateness of each resolution.

Because the self-assessment process may, in some cases, require considerable time to complete and approve, institutions should be aware of the expiration date of their cap resolutions well in advance. If a new cap resolution is not received by the expiration date, an institution may be assigned a zero cap, which would generally preclude the institution from using any Federal Reserve daylight credit.

Confidentiality

The Federal Reserve considers institutions' daylight-overdraft caps; cap categories; and collateralized capacity, if applicable, to be confidential information and will only share this information with an institution's primary supervisor. Institutions are also expected to treat cap and collateralized-capacity information as confidential. Cap and collateralized-capacity information should not be shared with outside parties or mentioned in any public documents.

DAYLIGHT-OVERDRAFT MONITORING AND CONTROL

All institutions that maintain Federal Reserve accounts and use Federal Reserve Services are expected to monitor their account balances on an intraday basis. Institutions should be aware of payments they are making from their accounts each day and how those payments are funded. Institutions are encouraged to use their own systems and procedures, as well as the available Federal Reserve's systems, to monitor their Federal Reserve account balance and payment activity.

Daylight-Overdraft Measurement

To determine whether a daylight overdraft has occurred in an institution's account, the Federal Reserve uses a set of transaction-posting rules that define explicitly the time of day that debits and credits for transactions processed by a Reserve Bank will post to the account.[11] All Fedwire funds transfers, book-entry securities transfers, and NSS transactions are posted to an institution's account as they occur throughout the day. Other transactions, including ACH and check transactions, are posted to institutions' accounts according to a defined schedule. These posting rules should help institutions control their use of intraday credit because they allow institutions to monitor the time that each transaction is credited or debited to their account. Note that these posting times affect the calculation of the account balance for daylight-overdraft-monitoring and pricing purposes but do not affect the finality or revocability of the entry to the account. An important feature of the posting rules is a choice of posting times for check credits.

Monitoring Daylight Overdrafts

To monitor an institution's overdraft activity and its compliance with the PSR policy and to calculate daylight-overdraft charges, the Federal Reserve uses the Daylight-Overdraft Reporting and Pricing System (DORPS). DORPS captures all debits and credits resulting from an institution's payment activity and calculates end-of-minute account balances using the daylight-overdraft posting rules. As measured by DORPS, an institution's account balance is calculated at the end of each minute, based on its opening balance and all payment transactions posted to the institution's account up until that moment. The daylight-overdraft measurement period begins with the current official opening time of

11. Posting rules were last amended on June 20, 2006, when the Board revised its PSR policy (effective July 20, 2006) concerning interest and redemption payments on securities issued by government-sponsored enterprises (GSEs) and certain international organizations. The revised policy requires Reserve Banks to release these interest and redemption payments as directed by the issuer, provided the issuer's Federal Reserve account contains sufficient funds to cover them. Each issuer is required to fund its interest and redemption payments by 4 p.m. eastern time for the payments to be processed that day. For further information on the posting rules, see the PSR policy.

Fedwire and continues until the official closing time. Although DORPS records positive as well as negative account balances, positive balances do not offset negative balances for purposes of determining compliance with net debit caps or for calculating daylight-overdraft fees. In cases of unscheduled extensions of Fedwire hours, the final closing account balance is recorded as if it was the balance at the standard closing time, and balances between the scheduled and actual closing times are not recorded. DORPS generates reports at the end of each two-week reserve-maintenance period.[12] These reports provide useful information for monitoring daylight overdrafts, such as peak daily overdrafts for the period; overdrafts in excess of net debit cap; end-of-minute account balances for a particular day; and related ratios, such as the peak daily overdraft relative to net debit cap.[13]

Monitoring PSR Policy Compliance

Reserve Banks generally monitor institutions' compliance with the PSR policy over each two-week reserve-maintenance period. In most cases, a policy violation occurs when an institution's account balance for a particular day shows one or more negative end-of-minute account balances in excess of its single-day net debit cap or when an institution's average peak daily overdraft over a reserve-maintenance period exceeds its two-week average cap.[14] The exceptions to this general rule are discussed below.

Institutions in the exempt-from-filing cap category are normally allowed two cap breaches in two consecutive, two-week, reserve-maintenance periods without violating the PSR policy. For institutions in all other cap categories or for institutions that have been approved for maximum daylight-overdraft capacity, each cap breach is considered a policy violation. A Reserve Bank may waive a violation in limited circumstances such as an operational problem at a Reserve Bank.

An institution with a self-assessed cap that has been approved for maximum daylight-overdraft capacity should avoid incurring daylight overdrafts that, on average over a two-week period, exceed its two-week-average limit, and that, on any day, exceed its single-day limit. The two-week-average limit is equal to the two-week average cap plus the amount of applicable collateralized capacity, averaged over a two-week reserve-maintenance period. The single-day limit is equal to an institution's net debit cap plus the amount of collateralized capacity.

For daylight-overdraft purposes, accounts of U.S. branches and agencies of foreign banks and accounts involved in merger-transitions are monitored on a consolidated basis; that is, a single account balance is derived by adding together the end-of-minute balances of each account. The accounts of affiliated institutions are monitored separately if they are separate legal entities. In addition, for institutions with accounts in more than one Federal Reserve District, an ARB is designated. The ARB coordinates the Federal Reserve's daylight-overdraft monitoring for the consolidated accounts or institutions.

Consequences of Violations

A PSR policy violation may initiate a series of Reserve Bank actions aimed at deterring an institution's excessive use of Federal Reserve intraday credit. These actions depend on the institution's history of daylight overdrafts and its financial condition. Initially, the Reserve Bank may assess the causes of the overdrafts, send a counseling letter to the institution, and review account-management practices. In addition, the Reserve Bank may require an institution to submit documentation specifying the actions it will take to address the overdraft problems. If policy violations continue, the Reserve Bank may take additional actions. For example, if a financially healthy institution in the zero, exempt-from-filing, or de minimis cap category continues to breach its cap, the Reserve Bank may recommend that the institution file a cap resolution or perform a self-assessment to obtain a higher net debit cap.

If an institution continues to violate the PSR policy, and if counseling and other Reserve Bank actions have been ineffective, the Reserve

12. Reserve Banks may make these reports available to institutions to assist in their internal account monitoring and control, and for the assessment of daylight overdraft fees.

13. For further information on the reports see the *Account Management Guide* at www.frbservices.org/Accounting/pdf/amg.pdf.

14. An institution's average peak daily overdraft is calculated by adding the largest overdraft incurred for each day during a reserve-maintenance period and dividing that sum by the number of business days in the period.

Bank may assign the institution a zero cap. In addition, the Reserve Bank may impose other account controls that it deems prudent, such as requiring increased clearing balances; rejecting Fedwire funds transfers, ACH credit originations, or NSS transactions in excess of the available account balance; or requiring the institution to fund certain transactions in advance. Reserve Banks also keep institutions' primary regulators apprised of any recurring overdraft problems.

Real-Time Monitoring

The Account Balance Monitoring System (ABMS) is the system Reserve Banks use to monitor in real time the payment activity of institutions that potentially expose the Federal Reserve and other payment-system participants to excessive risk exposure. ABMS is both an information source and an account-monitoring and control tool. It allows institutions to obtain intraday balance information for purposes of managing their use of daylight credit and avoiding overnight overdrafts. All institutions that have an electronic connection to the Federal Reserve's Fedwire funds-transfer service, such as a FedLine® terminal or a computer interface connection, are able to review their intraday Federal Reserve account position in ABMS. While ABMS is not a substitute for an institution's own internal tracking and monitoring systems, it does provide real-time account information based on Fedwire funds and securities transfers and NSS transactions. Additionally, ABMS captures debits and credits resulting from other payment activity as those transactions are processed in the Reserve Bank's accounting system. ABMS also provides authorized Federal Reserve Bank personnel with a mechanism to monitor and control account activity for selected institutions.

ABMS has the capability to reject or intercept funds transfers from an institution's account. This capability is called *real-time monitoring.* The Federal Reserve Banks use real-time monitoring to prevent selected institutions from transferring funds from their accounts if there are insufficient funds to cover the payments. Institutions are generally notified before a Reserve Bank begins monitoring their account in real time.

If an institution's account is monitored in the "reject" mode in ABMS, any outgoing Fedwire funds transfer, NSS transaction, or ACH credit origination that would cause an overdraft above a specified threshold, such as the institution's available funds, would be immediately rejected back to the sending institution. The institution could then initiate the transfer again when sufficient funds became available in its account. If an institution's account is monitored in the "intercept" mode, sometimes referred to as the "pend" mode, outgoing funds transfers, NSS transactions, or ACH credit originations that would cause an overdraft in excess of the threshold will not be processed but will be held. These intercepted transactions will either be released by the Reserve Bank once funds are available in the institution's account or rejected back to the institution. Reserve Banks will normally be in direct contact with an institution in the event any of its funds transfers are intercepted.

Institutions can view Federal Reserve accounting information on the web through FedLine. The Account Management Information (AMI) application provides real-time access to intraday account-balance and daylight-overdraft balance information, detailed transaction information, and a variety of reports and inquiry services. Institutions can obtain information on accessing ABMS and AMI from any Federal Reserve Bank or in the *Account Management Guide*.

SPECIAL TYPES OF INSTITUTIONS

U.S. Branches and Agencies of Foreign Banks

Under the PSR policy, U.S. branches and agencies of foreign banks are typically treated the same as domestic institutions. However, several unique considerations affect the way in which the policy is applied to U.S. branches and agencies of foreign banks. In general, net debit caps for foreign banking organizations (FBOs) are calculated in the same manner as they are for domestic banks, that is, by applying cap multiples for one of the six cap categories to a capital measure. For U.S. branches and agencies of foreign banks, net debit caps on daylight overdrafts in Federal Reserve accounts are calculated by applying the cap multiples for each

cap category to the FBO's U.S. capital equivalency measure. U.S. capital equivalency is equal to the following:

- 35 percent of capital for FBOs that are financial holding companies (FHCs)
- 25 percent of capital for FBOs that are not FHCs and have a strength-of-support assessment (SOSA) ranking of 1[15]
- 10 percent of capital for FBOs that are not FHCs and are ranked a SOSA 2
- 5 percent of "net due to related institutions" for FBOs that are not FHCs and are ranked a SOSA 3.

U.S. branches and agencies of foreign banks that (1) wish to establish a non-zero net debit cap, (2) are an FHC, or (3) are ranked a SOSA 1 or 2 are required to file the Annual Daylight Overdraft Capital Report for U.S. Branches and Agencies of Foreign Banks (FR 2225). Granting a net debit cap or any extension of intraday credit to an institution is at the discretion of the Reserve Bank. If a Reserve Bank grants a net debit cap or extends intraday credit to a financially healthy FBO ranked a SOSA 3, the Reserve Bank may require such credit to be fully collateralized, given the heightened supervisory concerns associated with these FBOs.

As it does with U.S. institutions, the ARB must have the ability to assess regularly the financial condition of a foreign bank in order to grant the institution a daylight-overdraft cap other than zero. The ARB will generally require information regarding tier 1 and total risk-based capital ratios for the consolidated foreign bank. Accordingly, U.S. branches and agencies of foreign banks seeking a positive daylight-overdraft cap (exempt, de minimis, or self-assessment cap categories) should provide the ARB with capital ratios at the time the cap is established and annually thereafter. Workpapers for capital ratios need to be maintained at a designated U.S. branch or agency and are subject to review by the institution's primary supervisor. The Federal Reserve considers capital information provided to the ARB in connection with an institution's daylight-overdraft capacity to be confidential.

Effective March 26, 2009, a foreign bank that (1) is an FHC or (2) has a SOSA rating of 1 and has a self-assessed net debit cap may request from its Reserve Bank a streamlined procedure to obtain a maximum daylight overdraft capacity up to 100 percent times the net debit cap multiple. Also effective March 26, 2009, eligible foreign banks are granted a capital measure of 100 percent of capital for the purposes of calculating the deductible for daylight overdraft pricing.[16] The provision regarding the deductible will remain in effect until the implementation of the revised PSR policy, which eliminates the deductible for all institutions.

Allocation of Caps

The Federal Reserve monitors the daylight overdrafts of U.S. branches and agencies of foreign banks on a consolidated basis; that is, each foreign-bank family, consisting of all of the U.S. branches and agencies of a particular foreign bank, has a single daylight-overdraft cap. Intraday account balances of all the U.S. branches and agencies in a foreign-bank family are added together for purposes of monitoring against its daylight-overdraft cap, in the same way that the account balances of institutions with accounts in more than one Federal Reserve District are added together.

For purposes of real-time monitoring, however, a foreign bank that has offices in more than one District may choose to allocate a portion of its net debit cap to branches or agencies in Districts other than that of the ARB. Unless a foreign-bank family instructs otherwise, the Federal Reserve will assign the dollar value of the family's single-day daylight-overdraft cap to the branch or agency located in the District of the ARB. The foreign-bank family may indicate to the ARB the dollar amount of cap to be allocated to offices in other Districts. Any dollar

15. The SOSA ranking is composed of four factors: the FBO's financial condition and prospects, the system of supervision in the FBO's home country, the record of the home country's government in support of the banking system or other sources of support for the FBO, and transfer-risk concerns. Transfer risk relates to the FBO's ability to access and transmit U.S. dollars, which is an essential factor in determining whether an FBO can support its U.S. operations. The SOSA ranking is based on a scale of 1 through 3, with 1 representing the lowest level of supervisory concern.

16. A deductible is a calculated amount that is subtracted from an institution's daylight overdraft charges. In order to be eligible for the interim deductible, FBOs must request and receive Reserve Bank approval for a streamlined max cap and have unencumbered collateral pledged at all times to its Reserve Bank equal to or greater than the amount of the deductible. Some max caps received under the general procedure may also be eligible.

amount of the cap that is not allocated to offices in other Districts will be assigned to the branch or agency in the District of the ARB. Annually, a foreign bank should update or confirm its cap allocation to its ARB.

Nonbank Banks and Industrial Banks

Institutions subject to the Competitive Equality Banking Act of 1987 (CEBA), such as nonbank banks or certain industrial banks, may not incur daylight overdrafts on behalf of affiliates, except in three circumstances. First, the prohibition does not extend to overdrafts that are a result of inadvertent computer or accounting errors beyond the control of both the nonbank bank or industrial bank and its affiliate. Second, nonbank banks are permitted to incur overdrafts on behalf of affiliates that are primary U.S. government securities dealers, provided such overdrafts are fully collateralized. Third, overdrafts incurred in connection with an activity that is financial in nature are also permitted. A nonbank bank or industrial bank loses its exemption from the definition of bank under the Bank Holding Company Act if it permits or incurs prohibited overdrafts. In enforcing these restrictions, the Federal Reserve uses a separate formula for calculating intraday Federal Reserve account positions for these institutions.

Institutions with Federal Reserve Accounts and No Access to the Federal Reserve Discount Window

Under the PSR policy, institutions that have Federal Reserve accounts but lack regular access to the discount window are not eligible for a positive daylight-overdraft cap. Institutions that do not have regular access to the discount window include Edge and agreement corporations, bankers' banks that are not subject to reserve requirements, limited-purpose trust companies, government-sponsored enterprises (GSEs), and certain international organizations. Institutions that have been assigned a zero cap by their Reserve Banks are also subject to special considerations under the PSR policy because of the risks they pose. All of these institutions are strongly discouraged from incurring any daylight overdrafts and are subject to a penalty fee on any average daily overdraft incurred. If any such institutions were to incur an overdraft, however, the Reserve Bank would require it to pledge collateral sufficient to cover the peak amount of the overdraft for an appropriate period.

The penalty fee is intended to provide a strong incentive for these institutions to avoid incurring any daylight overdrafts in their Federal Reserve accounts. The penalty fee assessed is equal to the annual rate applicable to the daylight overdrafts of other institutions (36 basis points) plus 100 basis points multiplied by the fraction of a 24-hour day during which Fedwire is scheduled to operate (currently 21.5 divided by 24). The daily overdraft penalty fee is calculated by dividing the annual penalty rate by 360. The daylight-overdraft penalty rate applies to the institution's average daily daylight overdraft in its Federal Reserve account. Institutions that are subject to the daylight-overdraft penalty fee are subject to a minimum penalty fee of $25 on any daylight overdrafts incurred in their Federal Reserve accounts.

SPECIAL SITUATIONS

Edge Act and Agreement Corporations

Edge Act and agreement corporations[17] do not have regular access to the discount window and should refrain from incurring daylight overdrafts in their Federal Reserve accounts. If any daylight overdrafts occur, the Edge Act or agreement corporation will be required to post collateral to cover them. Like foreign banks, Edge Act and agreement corporations that have branches in more than one Federal Reserve District are monitored on a consolidated basis. In addition to posting collateral, the Edge or agreement corporation would be subject to the daylight-overdraft penalty rate levied against the average daily daylight overdrafts incurred by the institution.

Bankers' Banks

Bankers' banks[18] are exempt from reserve

17. These institutions are organized under section 25A of the Federal Reserve Act (12 USC 611–631) or have an agreement or undertaking with the Board of Governors under section 25 of the Federal Reserve Act (12 USC 601–604a).

18. For the purposes of the PSR policy, a bankers' bank is a financial institution that is not required to maintain reserves

requirements and do not have regular access to the discount window. Bankers' banks may voluntarily waive their exemption from reserve requirements, thus gaining access to the discount window. These bankers' banks would then be free to establish caps and would be subject to the PSR policy in the same manner as other institutions. Bankers' banks that have not waived their exemption from reserve requirements should refrain from incurring overdrafts and must post collateral to cover any daylight overdrafts that they incur.

Limited-Purpose Trust Companies

The Federal Reserve Act (FRA) permits the Board to grant Federal Reserve membership to limited-purpose trust companies,[19] subject to conditions the Board may prescribe pursuant to the FRA. Limited-purpose trust companies that maintain Federal Reserve accounts should refrain from incurring overdrafts and must post collateral to cover any daylight overdrafts that they incur.

Government-Sponsored Enterprises and Certain International Organizations

The Federal Reserve Banks act as fiscal agents for certain government-sponsored enterprises (GSEs) and international organizations.[20] These institutions generally have Federal Reserve accounts and issue securities over the Fedwire Securities Service. The securities of these institutions are *not* obligations of, or fully guaranteed as to principal and interest by, the United States. Furthermore, these institutions are not subject to reserve requirements and do not have regular access to the discount window. GSEs and certain international organizations are to avoid incurring daylight overdrafts and must post collateral to cover any daylight overdrafts they do incur. In addition to posting collateral, these institutions are subject to the same daylight-overdraft penalty rate as other institutions that do not have regular access to the discount window.

Problem Institutions

For institutions that are in weak financial condition, the Reserve Banks will impose a zero cap. The Reserve Bank will also monitor a problem institution's activity in real time and reject or delay certain transactions that would create an overdraft. Problem institutions should refrain from incurring daylight overdrafts and must post collateral to cover any daylight overdrafts they do incur.

ELECTRONIC FUNDS TRANSFER ACTIVITIES

EFT MANAGEMENT

Economic and financial considerations have led financial institutions and their customers to recognize the need to manage cash resources more efficiently. The PSR policy calls on private networks and institutions to reduce their own credit and operational risks. It also depends on the role of the Federal Reserve and other financial institution regulators in examining, monitoring, and counseling institutions. To ensure that banking institutions are following prudent banking practices in their funds-transfer activities, examinations should focus equally on the

under the Federal Reserve's Regulation D (12 CFR 204) because it is organized solely to do business with other financial institutions, is owned primarily by the financial institutions with which it does business, and does not do business with the general public and is not an institution as defined in the Federal Reserve's Regulation A (12 CFR 201.2(a)). For the purposes of the PSR policy, bankers' banks also include corporate credit unions.

19. For the purposes of the PSR policy, a limited-purpose trust company is a trust company that, because of limitations on its activities, does not meet the definition of "depository institution" in section 19(b)(1)(A) of the Federal Reserve Act (12 USC 461(b)(1)(A)).

20. The GSEs include Fannie Mae, the Federal Home Loan Mortgage Corporation (Freddie Mac), entities of the Federal Home Loan Bank System (FHLBS), the Farm Credit System, the Federal Agricultural Mortgage Corporation (Farmer Mac), the Student Loan Marketing Association (Sallie Mae), the Financing Corporation, and the Resolution Funding Corporation. The international organizations include the World Bank, the Inter-American Development Bank, the Asian Development Bank, and the African Development Bank. The Student Loan Marketing Association Reorganization Act of 1996 requires Sallie Mae to tbe completely privatized by 2008; however, Sallie Mae completed privatization at the end of 2004. The Reserve Banks no longer act as fiscal agents for new issues of Sallie Mae securities, and Sallie Mae is not considered a GSE.

evaluation of credit, liquidity, and operational risks.

The bank should establish guidelines for types of allowable transfers. Procedures should be in effect to prevent transfers drawn against uncollected funds. Thus, banks should not transfer funds against simple ledger balances unless preauthorized credit lines have been established for that account.

Errors and omissions, as well as the fraudulent alteration of the amount of a transfer or of the account number to which funds are to be deposited, could result in losses to the bank. Losses may include total loss of the transferred funds, loss of availability of funds, interest charges, and administrative expenses associated with the recovery of the funds or correction of the problem.

Management is responsible for assessing the inherent risks in the EFT system, establishing policies and controls to protect the institution against unreasonable exposures, and monitoring the effectiveness of safeguards. Regulatory agencies will ensure that each financial institution has evaluated its own risks realistically and has adequate accounting records and internal controls to keep exposures within reasonable, established limits.

The risks associated with any computerized EFT system can be reduced if management implements the controls that are available on the system. For example, the authority to enter, verify, and send transfers can be segregated, and the dollar amount of transactions can be limited. Effective risk management requires that management establish and maintain—

- reasonable credit limits (payments in excess of these limits that involve significant credit risk must be properly approved by appropriate lending authorities),
- adequate recordkeeping to determine the extent of any intraday overdrafts and potential overnight overdrafts before releasing payments, and
- proper monitoring of respondents' accounts when the institution sets the positions of others. Responsibility for this function should be assigned to an appropriate supervisory level of management that will ensure the use of adequate internal controls.

Authentication or Verification Methods

The same due care that financial institutions use when executing EFT transactions must be used when accepting EFT requests from customers. Management must implement security procedures for ensuring that the transfer requests are authentic. As stated in Uniform Commercial Code (UCC) section 4A-201, "Authorized and Verified Payment Orders," security procedures may require the use of algorithms or other codes, identifying words, or numbers; encryption; callback procedures; or similar security devices. An explanation of authorized and verified payment orders is detailed in UCC section 4A-202.

Signature Verification

One method to verify the authenticity of a customer's EFT request is to verify the customer's signature. Unfortunately, this procedure cannot be performed when the customer requests the transaction by telephone. Some financial institutions have implemented policies whereby the customer completes and signs a transfer request, and then faxes the request to the bank. However, this is not a safe EFT procedure because, although the bank can verify the signature on the faxed request, it cannot be certain that the transfer request is legitimate. Any document that is transmitted electronically can be altered (for example, by changing the amount or account number). The alteration can occur before the document is digitalized (that is, before being fed into the fax machine) or after. In most instances, these alterations cannot be detected by the receiving entity. If there is any question about a document's authenticity, the transaction should be reconfirmed through other sources.

Personal Identification Numbers

One way for financial institutions to authenticate transfers initiated over the telephone is through the use of personal identification numbers (PINs) issued to each customer. When a customer requests a transfer, his or her identity is verified by comparing the supplied PIN with the customer's PIN-request form that is on file. At a

minimum, the following safeguards should be implemented for these types of transfers:

- All nonretail customers should be requested to sign an agreement whereby the bank is held harmless in the event of an unauthorized transfer if the bank follows routine authentication procedures. The customer is responsible for informing the bank about changes in who is authorized to execute EFTs. These procedures should minimize the risk to the bank if someone is able to execute a fraudulent transaction. (These procedures are described in detail in UCC section 4A-202.)
- All transactions over a specific dollar amount should be re-verified by a callback routine. The bank should require that the person being called for re-verification is someone other than the person who initially requested the transaction.
- Whenever new PINs are issued, they should be mailed in sealed, confidential envelopes (preferably computer-generated) by someone who does not have the ability to execute wire transfers.
- The number of bank employees who have access to PINs should be very limited.

Tape Recording

The tape recording of EFT requests made over the telephone is another internal control practice. When possible, verifying and recording the incoming telephone number (that is, using a caller-ID system) is also a good practice. The laws addressing telephone recording vary by state. Some states require that the caller be informed that the conversation is being recorded; others do not have this requirement. Regardless of the state's law, the bank should inform callers that, for their protection, conversations are being recorded. Moreover, banks should have in place a policy for archiving the taped telephone records and should retain them for a specified period of time, at least until the statements from the Federal Reserve or correspondent banks have been received and reconciled.

Statements of Activity

Some larger banks have implemented a procedure whereby customers are electronically sent a summary statement at the end of each day. The statement lists the transfers executed and received on their behalf. The statement can be sent through a fax machine, a personal computer, or a remote printer. This procedure quickly identifies any transfers the customer did not authorize.

Test Keys

EFT requests can be authenticated using *test keys.* A test key is a calculated number that is derived from a series of codes that are contained in a test-key book. The codes in a test-key book represent such variables as the current date, hour of the day, receiving institution, receiving account number, and amount of the transfer. The value derived from these variables equals the test key. The financial institution or corporate customer initiating the transfer will give its EFT information, along with the test-key value. The receiving bank will recalculate the test key and, if the two test keys equal the same amount, the EFT request is considered authenticated. Test-key code books should be properly secured to prevent unauthorized access or fraudulent use. The use of test keys has declined in recent years as more and more institutions implement PC-based EFT systems.

Blanket Bond

Although computer-related employee misappropriations are normally covered, financial institution blanket bond policies generally exclude certain types of EFT activities from standard coverage. Separate coverage for EFT systems is available and should be suggested to management, particularly if a significant risk exposure exists. A bank's fidelity bond insurance could be declared null and void by the carrier if a fraudulent transfer were to occur and the loss was directly attributable to weak internal controls. (See section 4040.1, "Management of Insurable Risks.")

SUPERVISORY RISK EVALUATION

Bank management is responsible for assessing the inherent risks in the EFT system (or

systems) it uses. Management should establish policies and controls to protect the institution against unreasonable exposures, as well as monitor the effectiveness of the established safeguards.

Examiner Responsibilities

Examiners are responsible for ensuring that financial institutions have assessed and evaluated their risks realistically and have adopted internal controls that are adequate to keep those risks within acceptable limits. The types of risks involved in EFT systems, as well as payment systems generally, are discussed below.

Credit Risk

Credit risk is the risk that a counterparty will not settle an obligation for full value when due, nor at any time subsequently. Any time an institution extends credit to a customer or permits a customer to use provisional funds to make a payment, the institution is exposed to the risk that the customer will not be able to meet its payment obligation. If the customer is unable or unwilling to repay the credit extension, the institution could incur a financial loss. Similarly, an institution that receives a payment in provisional funds has a credit exposure to the sender until such time as the payment is settled with finality, that is, until the payment becomes unconditional and irrevocable. If an institution permits a customer to withdraw or make a payment with provisional funds received, then the institution incurs credit exposure to both the sender of the provisional funds and the customer. Those credit exposures are not extinguished until the provisional funds received are settled with finality. With respect to payment systems risk, overall credit risk consists of (1) direct-credit risk to the Federal Reserve, that is, a borrowing institution may be unable to cover its intraday overdraft arising from a transfer of funds or receipt of book-entry securities, thus causing a Federal Reserve Bank to incur a loss; (2) private direct-credit risk, or the possibility of loss to institutions extending credit; and (3) systemic risk, which is the possibility of loss to multiple creditors when borrowing institutions fail to cover their obligations to creditor institutions. Variants of credit risk include sender risk, receiver risk, and return-item risk.

Systemic risk. Stated more clearly, systemic risk occurs when one participant in a payment system, or in the financial markets generally, fails to repay its required obligation when due, and this failure prevents other private or market participants or financial institutions from meeting their settlement obligations when due. Systemic risk may result from extraneous events, actions, or reasons that are independent of the institution, or from developments in the payment system. Changes in the capital markets, domestic political or government announcements or actions, unplanned events, or sovereign actions of other countries are examples of events that may cause systemic risk.

Sender risk. Sender risk is the risk that results if a depository institution uses an extension of credit to make an irrevocable payment on behalf of a customer. This credit can be a loan or an extension of payment against uncollected or provisional funds or against insufficient balances.

Receiver risk. Receiver risk arises when an institution accepts funds from a sender who may be a customer, another institution, or the payment system. As the receiver of funds, the institution relies on the sender's ability to settle its obligations. The risk exists while payments are revocable within the system and remains until final settlement.

Return-item risk. The major risk in originating ACH debit transactions and collecting checks for customers is return-item risk. Return-item risk extends from the day funds are made available to customers until the individual items can no longer legally be returned. The receiver of ACH debit transactions, or the payer of checks, has the right to return transactions for various reasons, including insufficient funds in its customer's account. To minimize its exposure, an institution should perform credit assessments of all customers that originate large dollar volumes of ACH debit transactions, and for all customers for which the institution collects large volumes of checks. Such assessments ensure that if ACH or check items are returned after the customer has been granted use of the funds, the customer will be able to return the funds to the institution.

Liquidity Risk

Liquidity risk is the risk that a counterparty will not settle an obligation for full value when due, even though the counterparty may later settle the obligation. Liquidity risk may result from unexpected market or operational disruptions or from catastrophic or unplanned events. It may also result from sovereign actions; therefore, sovereign risk can give rise to liquidity risk.

Sovereign Risk

Sovereign risk refers to the financial capacity of governments to generate foreign-currency revenues to repay their obligations. This capacity is generally limited because government assets are predominantly the discounted value of future taxes denominated in the local currency. Governments have direct access to foreign-currency revenues only when the economy is dominated by a public sector that derives most of its revenues from exports (for example, oil or gold). Sovereign risk is not limited to the country's federal government debt. It also includes debt contracted by all public and publicly guaranteed entities (such as provincial, state, or local governments and all other debt with a government's guarantee).

Actions taken by nondomestic governments can affect the payments of certain participants in a payment system, and these actions can be detrimental to other participants in the system. Sovereign risk can include the imposition of exchange-control regulations on a bank participating in international foreign-exchange activities. While the bank itself may be both willing and able to settle its position, government intervention may prevent it from doing so. The risk can be controlled by regularly monitoring the payment-system laws of other countries and by taking specific alternative actions to lessen the risk. Alertness to a bank's sovereign-risk exposure to its counterparties located in other nations, and to possible alternative actions, can considerably lessen this risk.

Legal Risk

Any transaction occurring in a payment system is subject to the interpretation of courts in different countries and legal systems. This issue is normally addressed by adopting "governing-law" provisions in the rules of the systems themselves. These provisions provide for all disputes between members to be settled under the laws of a specific jurisdiction. However, if a local court refuses to recognize the jurisdiction of a foreign court, the rules may be of limited use. This risk is difficult to address because there is no binding system of international commercial law for electronic payments. Banks should seek a legal opinion regarding the enforceability of transactions settled through a particular system.

Operational Risk

Operational risk may arise from—

- a system failure caused by a breakdown in the hardware or software supporting the system, possibly resulting from design defects, insufficient system capacity to handle transaction volumes, or a mechanical breakdown, including telecommunications;
- a system disruption if the system is unavailable to process transactions, possibly due to system failure, destruction of the facility (from natural disasters, fires, or terrorism), or operational shutdown (from employee actions, a business failure, or government action); or
- the system being compromised as a result of fraud, malicious damage to data, or error.

Whatever the source, the loss of availability of a payment system can adversely affect major participants, their correspondents, markets, and interdependent payment mechanisms.

Banks should control operational risk through a sound system of internal controls, including physical security, data security, systems testing, segregation of duties, backup systems, and contingency planning. In addition, a disruption to a bank's own internal payment processing systems or its access to external payment systems can adversely affect both the bank's own payments activities, as well as those of other participants in a payment system. As such, a comprehensive audit program is essential to assess the risks, adequacy of controls, and compliance with bank policies.

Risk-Control Issues

Bank management should consider and develop risk-management policies and procedures to address the variety of credit, liquidity, operational, and other risks that can arise in the normal course of conducting its payment business—regardless of the clearing and settlement method of the particular payment systems in which the bank participates. EFT systems differ widely in form, function, scale, and scope of activities. Consequently, the specific risk-management measures an institution employs for a particular EFT system will differ depending on the inherent risks in the system. As a general matter, an institution should adopt risk-management controls commensurate with the nature and magnitude of risks involved in a particular EFT system.

In addition to assessing the adequacy of an institution's risk-management procedures for measuring, monitoring, and controlling its risks from participating in a payment system (or systems) and from providing payment services to its customers, examiners should consider the following internal control guidelines when they review policies and procedures covering EFT activities:

- Job descriptions for personnel responsible for a bank's EFT activities should be well defined, providing for the logical flow of work and adequate segregation of duties.
- No single person in an EFT operation should be responsible for all phases of the transaction (that is, for data input, verification, and transmission or posting).
- All funds transfers should be reconciled at the end of each business day. The daily balancing process should include a reconciliation of both the number and dollar amount of messages transmitted.
- All adjustments required in the processing of a transfer request should be approved by a bank's supervisory personnel, with the reasons for the adjustment documented. Transfer requests "as of" a past or future date should require the supervisor's approval with well-defined reasons for those requests.
- Only authorized persons should have access to EFT equipment.

Considerable documentation is necessary to maintain adequate accounting records and auditing control. Many banks maintain transfer-request logs, assign sequence numbers to incoming and outgoing messages, and keep an unbroken electronic copy of all EFT messages. At the end of each business day, employees who are independent of the transfer function should compare request forms with the actual transfers to ensure that all EFT documents are accounted for. When reviewing the adequacy of internal controls, examiners should review the funds-transfer operations to determine that recordkeeping systems are accurate and reliable, all transactions are handled promptly and efficiently, duties are separated appropriately, audit coverage is adequate, and management recognizes the risks associated with these activities.

1. To determine if the bank's electronic funds transfer (EFT) objectives, policies, practices, procedures, and internal controls are adequate to control its exposure to acceptable limits of payment systems risk.
2. To determine if bank officers and other wire-transfer personnel are operating in conformance with established guidelines.
3. To determine the scope and adequacy of the audit function for the risks associated with payment and wire-transfer systems.
4. To ascertain whether senior management is informed of the current status, nature, and magnitude of risks associated with the bank's EFT operations, as well as any changes to these risks.
5. To assess the bank's ability to monitor its payment-systems position, as well as to limit its credit and other risk exposures in the system and from its customers or correspondents.
6. To determine that the board of directors has reviewed and approved the institution's use of Federal Reserve intraday credit, self-assessment (if applicable), and net debit cap, and to determine if the institution is complying with the Federal Reserve Policy Statement on Payments System Risk.
7. If the bank has a self-assessed net debit cap, to review the bank's self-assessment file and determine if the underlying analyses and methodologies are reasonable, adequate, and consistent with the institution's supervisory overview, risk assessments, and risk matrix.
8. To evaluate the quality of the bank's operational controls and determine the extent of compliance with applicable laws and regulations.
9. To initiate corrective action when objectives, policies, procedures, or internal controls are deficient or when violations of law or regulations exist.

1. Review and determine the bank's compliance with the electronic funds transfer (EFT) risk-assessment standards of the examination module, recognizing the associated risks for each. Answer the pertinent questions that refer to EFT in the internal control questionnaire.
2. Review and evaluate the work of internal or external auditors and of the compliance officer as it relates to the risks associated with payment systems and EFT activities. Determine if payment system risk is reviewed and whether the independence, scope, coverage, and frequency of internal or external reviews are adequate.
3. Based on an evaluation of internal controls and the work performed by internal or external auditors, determine the scope of the examination.
4. Test for compliance with policies, practices, procedures, and internal controls. Determine whether the management information systems and reports for the institution's payment systems and funds-transfer activities provide timely and accurate data that are sufficient for personnel to make informed and accurate decisions. From the examiner assigned to review "Internal Control," obtain a listing of any deficiencies noted in the latest review conducted by internal or external auditors. Determine if bank management has taken the appropriate corrective actions for the deficiencies.
5. Obtain or construct an organizational chart and flow chart for the EFT area, and determine the job responsibilities and flow of work through that department.
6. Review the bank's standard form of agreement or other written agreements with its customers, correspondent banks, and vendors. Determine whether those agreements are current and clearly define the liabilities and responsibilities, including responsibilities during emergencies, of all parties. Agreements with the Federal Reserve Bank should refer specifically to the operating circular (or circulars) on the electronic funds transfers pursuant to subpart B of Regulation J (12 CFR 210.25 et seq.).
7. Review the bank's board of directors and senior management policies and procedures for payment-systems and EFT activities, including third-party transactions. Perform tests to determine the existence, reasonableness, and adequacy of these policies and procedures. Determine whether the policies and procedures have been disseminated to the employees who are actively responsible for and involved in performing payment-systems and EFT activities. Ascertain whether there is an active employee-training program that ensures employees have the knowledge necessary to comply with the bank's policies and procedures for payment-systems and EFT activities.
8. For transactions involving the Federal Reserve Bank, other private funds-transfer systems, and other due from bank accounts, confer with the examiner who is assigned "Due from Banks," and determine the propriety of any outstanding funds-transfer items.
9. Coordinate the review of the credit exposures arising from payment-systems and EFT activities with the examiners' review of loan programs or loan portfolios. Determine whether credit personnel make and adequately document, independent of account and operations officers, periodic credit reviews of funds-transfer customers.
10. Determine where suspense items or adjustment accounts are posted and accounted for, as well as who is responsible for reviewing, resolving, and clearing out suspense items.
    a. Scan accounts for unusual or old items or abnormal fluctuations.
    b. Reconcile accounts to departmental control totals and to the general ledger.
    c. Review management reports on suspense items and unusual activity.
11. Review the income and expense accounts related to EFT operations. Determine the frequency of entries caused by late or inaccurate execution of transfer requests.
12. Observe the space and personnel allocated to the EFT area, and note the location of communications terminals. Determine whether existing conditions are adequate to provide appropriate physical security.
13. Discuss the following items with the appropriate officer (or officers), and prepare summaries in the appropriate section of the

examination report:

a. internal control exceptions, as well as deficiencies in or noncompliance with written policies, practices, and procedures
b. uncorrected audit deficiencies
c. violations of laws and regulations
d. terminology, operating arrangements, accounting procedures, and time limitations of EFT operations
e. the operating efficiency and physical security of the bank's EFT operation
f. the adequacy of controls over settlement- and credit-risk exposure
g. recommended corrective action when policies, practices, or procedures are deficient

14. Update the examination workpapers to include the bank examination activities and procedures performed and any information gathered to support the completed work, including any information that will facilitate future examinations.

RISK MANAGEMENT OF INTRADAY CREDIT EXPOSURES

1. If the bank is a CHIPS or other clearing-agency participant, determine the bank's basis for accepting customers for CHIPS-payments activity. If the examined institution is a funding participant on CHIPS, determine the criteria for accepting a nonfunding participant as a respondent. Determine that the criteria are reviewed periodically.
2. Determine if appropriate intraday credit limits are imposed and monitored for those customers and counterparties with which the bank has intraday credit exposures.
3. Determine if the bank monitors and controls any intraday credit exposures to affiliates.[1]
4. Determine whether the institution periodically reviews its ability to fund its closing-position requirement on private multilateral settlement systems, such as CHIPS.

FEDERAL RESERVE INTRADAY CREDIT

1. Determine that the board of directors has reviewed and approved the institution's use of Federal Reserve intraday credit.
2. If the institution incurs daylight overdrafts in its Federal Reserve account, determine that the institution has selected an appropriate net debit cap.
3. If the institution has selected a de minimis or a self-assessed net debit cap, determine that the board-of-directors resolution follows the prescribed format and contains all of the required elements.
4. If the institution has selected a self-assessed net debit cap, review the contents of the self-assessment file to determine that the institution has applied the guidelines appropriately and diligently, that the underlying analysis and method were reasonable, and that the resulting self-assessment is generally consistent with the examination findings. Inform the appropriate Reserve Bank of any concerns about the institution's net-debit-cap level, self-assessment, or use of Federal Reserve intraday credit.
5. Review the institution's cap resolution file and ascertain that it includes (1) a copy of the board-of-directors resolution, (2) worksheets and supporting analysis used in its self-assessment of its own cap category, (3) copies of senior-management reports to the board of directors of the institution or its parent (as appropriate) regarding that self-assessment, and (4) copies of the minutes of the discussion at the appropriate board-of-directors meeting concerning the institution's adoption of a cap category.

1. An insured depository institution must establish and maintain policies and procedures reasonably designed to manage the credit exposure arising from its intraday extensions of credit to affiliates in a safe and sound manner. The policies and procedures must at a minimum provide for the monitoring and control of the credit exposure arising from the institution's intraday extensions of credit to each affiliate and all affiliates in the aggregate, and must ensure that the institution's intraday extensions of credit to affiliates comply with section 23B of the Federal Reserve Act. (See 12 CFR 250.248.)

For the preliminary review and assessment, review the bank's internal controls, policies, practices, and procedures for payment systems risk and electronic funds transfer (EFT) activities. The following procedures should be used:

1. Review previous examination reports, earlier workpapers, and correspondence exchanged with the institution to get an overview of previously identified EFT concerns.
2. Review the most recent audits and internal reviews to identify the scope and noted deficiencies.
3. Review management's actions to correct examination and audit deficiencies.
4. Discuss with management recent or planned changes in EFT activities.
5. Review management reports to determine the nature and volume of current activity.
6. Review the minutes of management committees that oversee EFT activity to determine their content and follow-up on material matters.

The bank's payment and EFT systems should be further reviewed and documented completely and concisely. Where appropriate, the preliminary review and assessment should include narrative descriptions, flowcharts, copies of forms used, and other pertinent information.

During the examination, the review of operations and internal controls of all institutions involved in funds-transfer or EFT activities should use the following procedures. Items below that are marked with an asterisk (*) require substantiation by observation or testing.

ORGANIZATION

1. Is there a current organization plan detailing the structure of the funds-transfer function?
2. Is senior management responsible for administering the operations of the funds-transfer function?
3. Does management maintain a current list of bank personnel who are authorized to initiate EFT requests?
4. Are there regular management reviews of staff compliance with the credit and personnel procedures, operating instructions, and internal controls?
5. Are activity and quality-control reports received and reviewed by management?
6. Are major new system designs and newly available hardware for the payment and EFT systems brought to the attention of and reviewed by management?

SUPERVISION BY DIRECTORS AND SENIOR MANAGEMENT

1. Are the directors and senior management kept informed about the nature and volume of transactions and the magnitude of the risks involved in the funds-transfer activity?
2. Has the board of directors or senior management reviewed and approved any limits on the risks in the funds-transfer activities? If so, when were the limits last reviewed?
3. Is senior management or the board of directors advised of any customers with—
   a. large intraday and overnight overdrafts? If so, are other extensions of credit to the same customers combined to show the total credit exposures?
   b. large drawings against uncollected funds?
4. Are management's responses to audit exceptions and recommendations adequate and timely?
5. Is there adequate insurance coverage for EFT risks? Does senior management conduct adequate reviews of insurance coverage and insurance riders for EFT operations and the overall EFT environment?

CREDIT MANAGEMENT, EVALUATION, AND APPROVAL

1. Under the bank's established board-of-directors policies and procedures, is senior management or the credit committee (or credit officers) required to review at predetermined frequencies—

   a. the volume of transactions, the creditworthiness of customers, and the risks involved in the funds-transfer activity?
   b. credit and other exposures as they relate to safe and sound banking practices?
   c. staff capabilities and the adequacy of equipment relative to current and expected volume?
2. Are procedures in place to prohibit transfers of funds against accounts that do not have collected balances or preauthorized credit availability?
3. Have counterparty and customer credit limits been established for all payment system risk exposures, including those relating to Fedwire, CHIPS, ACH, foreign exchange, and other types of payments? Do credit limits take into account intraday and overnight overdrafts?
   a. Are groups of affiliated customers included in such limits?
   b. Are limits set according to a clear and consistent methodology for credit-risk assessment?
   c. How often are the limits reviewed and updated?
   d. Does senior management monitor and review the customer limits? How frequently?
4. Are other types of credit facilities considered when establishing intraday-overdraft limits for the same customer?
5. Is an intraday-posting record kept for each customer, showing opening collected and uncollected balances, transfers in, transfers out, and the collected balances at the time payments are released?
6. If payments exceed the established limits, are steps taken in a timely manner to obtain covering funds?
7. Are there fully documented, periodic credit reviews of funds-transfer customers?
8. Are credit reviews conducted by competent credit personnel who are independent of account and operations officers?
9. Does the institution make payments in anticipation of receiving covering funds? If so, are such payments approved by officers who have the appropriate credit authority?
10. Are intraday exposures limited to amounts that are expected to be received the same day?
11. Do the limits on intraday and overnight overdrafts appear to be reasonable in view of the institution's capital position and the creditworthiness of the respective customers?
12. Does a staff supervisor approve payments in excess of established limits, following verification that the covering funds are in transit to the bank?
13. Before releasing payments, are payments against uncollected funds and intraday overdrafts in excess of established limits referred to a person with appropriate credit authority for approval, and is the reason for the overdraft determined?

PERSONNEL

1. Has the bank taken steps to ensure that screening procedures are applied to personnel that are hired for sensitive positions in the EFT departments?
2. Does the bank prohibit new or temporary employees from working in sensitive areas of the payment-systems and EFT operation?
3. Are statements of indebtedness required from employees who work in sensitive positions of the payment-systems and EFT function?
4. Does supervisory staff give special attention to employees newly assigned to work in the EFT functions?
5. Are employees subject to unannounced rotation of responsibilities, regardless of the size of the institution?
6. Are relatives of employees in the payment-systems and EFT function precluded from working in the same institution's bookkeeping or data processing departments?
7. Does the bank's policy require that employees take a minimum number of consecutive days as part of their annual vacation? Is this policy being enforced?
8. If employees have given notice of resignation or received termination notices, does management reassign them away from sensitive areas of the payment-systems and EFT function?
9. Are personnel informed of the current trends in transfer activities, including necessary internal controls, as part of a regular training program?

SIGNATURE CARDS

1. Does the bank maintain a current list or card file of authorized signers for customers who use the bank's funds-transfer services?
2. Are customer signature cards maintained under dual control or otherwise protected?
3. Do customer signature cards limit the number of authorized persons and the amount of funds that an individual is authorized to transfer?
4. Do bank personnel compare the signature on an original mail request with the authorized signature on file?

TEST KEYS

1. Do telephone requests and EFT transactions use test codes, and are the codes verified by a person other than the person receiving the request?
2. Are test codes restricted to authorized personnel?

*3. Are the files containing test-key formulas maintained under dual control or otherwise protected?

4. Are only authorized personnel permitted in the test-key area or allowed access to computers, teletapes, or terminals?
5. Does the bank maintain an up-to-date test-key file?
6. Does management maintain a list of those authorized persons who have access to test-key files?
7. Are all messages and transfer requests that require testing authenticated by the use of a test key?

*8. Are test codes verified by someone other than the person receiving the initial transfer request?

9. Are callback or other authentication procedures performed on all transfers that do not have a test key or signature card on file?
10. Do mail transfer requests include a test word as an authentication procedure?
11. Does the bank's test-key formula incorporate a sequence number resulting from an agreement between the bank and the customer?
12. Does the bank have procedures in operation for the issuance and cancellation of test keys?

*13. Is the responsibility for issuing and canceling test keys assigned to someone who is not responsible for testing the authenticity of transfer requests?

14. Are test codes maintained in a secure environment when they are not in use?
15. Is the testing area physically separated from other operations?

TELEPHONE TRANSFER REQUESTS

1. Has the bank established guidelines for what information should be obtained from a person making a funds-transfer request by telephone?
2. Does the above information include a test-word authentication code?
3. Does the bank use a callback procedure that includes a test-code authentication to verify telephone transfer requests?
4. Does the bank limit callbacks to transactions over a certain dollar amount?
5. Does the bank maintain a current list of persons who are authorized to initiate telephone funds transfers and messages?

*6. Does the bank have procedures in place to prohibit persons who receive telephone transfer requests from transmitting those requests?

7. Does the bank use devices that record all incoming and outgoing transfer requests?
8. Are prenumbered or sequentially numbered (at a central location after initiation) transfer-request forms used?
9. Is the log or record of transfer requests reviewed daily by supervisory personnel?
10. Do the records of transfer requests contain—
    a. a sequence number?
    b. an amount transferred?
    c. the person, firm, or bank making the request (also the specific transferor)?
    d. the date?
    e. the test-code authentication?
    f. paying instructions?
    g. authorizing signatures for certain types and dollar-amount transfers?

EFT REQUESTS

*1. Do different employees perform the functions of receipt, testing, and transmission of funds-transfer requests?
2. Do incoming and outgoing messages record the time, or are they sequentially numbered for control?
3. Do incoming and outgoing messages include a test word as a means of message authentication?
4. Is an unbroken copy of all messages kept throughout the business day?
5. Is the above copy reviewed and controlled by someone not connected with operations in the EFT area?

AGREEMENTS

1. With respect to EFT and payment-systems transfer operations between the bank and its hardware and software vendors, maintenance companies, customers, correspondent banks, the Federal Reserve, and other providers, are the agreements in effect and current? (The agreements with the appropriate Federal Reserve Bank should refer to the operating circulars regarding the transfer of funds pursuant to subpart B of Regulation J.)
2. Do the written agreements state the responsibilities of each party involved in the agreement?
3. Do the agreements state the vendors' liabilities for their employees' actions?

OPERATING AND PROCESSING PROCEDURES

1. Do written procedures exist for the EFT functions, and are they updated for employees in the incoming, preparation, data entry, balance-verification, transmission, accounting, reconciling, and security areas? Do these procedures include—
   a. control over test words, signature lists, and opening and closing messages?
   b. computer-terminal security and password controls?
   c. access to the funds-transfer and EFT areas and user files?
   d. origination, modification, deletion, or rejection of order transactions or messages?
   e. verification of the sequence numbers of orders?
   f. accounting for all transfer requests and message traffic at the end of the day?
   g. bank supervisory review of all adjustments, reversals, and the reasons therefor, as well as open items?
   h. planning for contingencies?
2. Are all incoming and outgoing payment orders and message requests in the EFT and funds-transfer area—
   a. time-recorded or sequentially numbered for control?
   b. logged?
   c. reviewed for test verification?
   d. reviewed for signature authenticity?
   e. reviewed to verify that the person who initiated the funds-transfer request was authorized to do so?
   f. authorized or reviewed by bank supervisory personnel?
3. Does the EFT department of the bank prepare a daily reconcilement of funds-transfer activity by dollar amount and number of messages?
4. Are all rejects or exceptions reviewed by someone who is not involved in the receipt, preparation, or transmittal of funds?
5. If the institution accepts transfer requests after the close of business or accepts transfer requests with a future value date, are they properly controlled and processed?
6. Are Federal Reserve Bank statements reviewed and reconciled daily with the bank's internal funds-transfer log to determine if there are "open" funds-transfer items and the reasons for the outstanding items?
7. Does an officer review corrections, overrides, open items, reversals, and other adjustments?
8. Does a person other than the receipt clerk review message requests and payment orders for—
   a. the propriety of the transactions?
   b. future dates, especially those for multiple transactions?
9. When reasonably feasible, does a supervisor check all transactions before the release of funds to a customer or before initiating a payment message over the EFT system?

10. At the end of a day, are all message requests and payment orders accounted for in an end-of-the-day proof to ensure that all requests have been processed?
11. Are internally rejected customer transfer requests and message requests controlled, and are they sequentially numbered for accountability?
12. Does an officer review and approve as-of adjustments, open items, reversals, and other adjustments?
13. Are key fields re-verified before transmission, and are messages released by someone other than the individual who originally entered the message?
14. Does the work flow in a one-way direction to provide adequate internal controls?
15. Are audit trails maintained from receipt through posting to a customer's account?
16. Are EFT activities adequately documented, and is there an adequate and active records-retention program?

ACCOUNTING, RECORDKEEPING, AND CONTROLS

1. Are Federal Reserve Bank, correspondent bank, and clearinghouse statements used for funds transfers reconciled daily in another area of the bank (for example, accounting or correspondent banking or by a person who is separate from any money-transfer operations) to ensure that they agree with the funds-transfer records?
2. Are all prenumbered forms, including cancellations, accounted for in the daily reconcilement, and do they include the account number and account title?
3. Is the daily reconcilement of funds-transfer and message-request activity reviewed by supervisory personnel?

*4. Is the balancing of daily activity conducted separately from the receiving, processing, and sending functions?

5. Does the EFT department verify that work sent to other bank departments agrees with its totals?
6. Are general-ledger entries, adjustments, automated transactions, or other supporting documents initialed by authorized persons?
7. Does the institution receive cables or other written communications from its customers that indicate amounts to be paid and received and the source of covering funds?
8. If the above detail of receipts is not received, do the institution's customers inform it of the total amount to be received for the day?
9. Is the information in items 7 and 8 maintained and followed for exceptions?
10. Is an intraday-posting record kept for each customer, showing opening collected and uncollected balances, transfers in, transfers out, and the collected balance at the time payments are released?
11. Are significant CHIPs or Fedwire customer payments and receipts communicated to a monitoring unit promptly during the day to provide adequate information on each customer's overall exposure?
12. Does the accounting system for demand deposits give an accurate collected-funds position?
13. Have limits been established within which a designated person may authorize release of payments after reviewing the customer's activity? Does the institution maintain a record of approvals of these releases?
14. When an overnight overdraft occurs, is a determination made as to whether a fail caused the overdraft? If so, is this determination properly documented? Are follow-up actions to obtain the covering funds in a timely manner adequate?
15. Does the institution have a record of payments it failed to make?
16. Is the above record reviewed to evaluate the efficiency of the department?
17. Is corrective action initiated when appropriate?
18. Are investigations and follow-ups for failed payments conducted by personnel who are independent of the operating unit?
19. Are customer advices issued in a timely manner? Do credit advices sent to customers clearly indicate that credits to their accounts that are received through CHIPS are conditional upon final settlement?
20. For the settling institutions on CHIPS, are the net debit positions of the nonsettling participants relayed to appropriate personnel as soon as the positions become known?
21. Are designated supervisory staff responsible for verifying that respondents' net debit positions are covered the same day?
22. Are the follow-up procedures adequate to facilitate the receipt of funds?

23. Are open-statement items, suspense accounts, receivables, or payables and interoffice accounts related to EFT activity controlled outside of the funds-transfer operations?
24. Do the following controls exist?
    a. Management prepares periodic reports on open-statement items, suspense items, and interoffice accounts.
    b. Reports include agings of open items, the status of significant items, and the resolution of prior significant items.
25. Do general-ledger tickets or other supporting documents include the initials of the originator and designated supervisory personnel?
26. Is senior management required to decide whether to refuse to cover a net debit settlement position of a respondent?
27. Has the institution devised and maintained an adequate system of internal accounting controls, as required by the Foreign Corrupt Practices Act?

AUDIT

1. Does management or the audit department undertake a periodic review to ensure that work is being performed in accordance with policy and guidelines established by the board of directors and senior management?
2. Is the audit department promptly informed when a change is made in systems or the method of operation?
3. Does the audit or independent-review program provide sufficient coverage relative to the magnitude (volume) and nature of EFT activities? Are independent reviews conducted, and do they address all areas of EFT business, including—
    a. payment-order origination (funds-transfer requests);
    b. message testing;
    c. credit evaluation;
    d. customer agreements;
    e. payment processing and accounting;
    f. personnel policies;
    g. physical and data security;
    h. contingency plans;
    i. credit evaluation and approval;
    j. incoming funds transfers;
    k. bank secrecy and foreign assets control, if applicable; and
    l. Federal Reserve payment system risk program and policy issues.

PHYSICAL SECURITY

1. Is access to the EFT area restricted to authorized personnel who have proper bank identification? In limited circumstances when visitors are necessary (such as for repairs of equipment), are they restricted, properly identified, required to sign in, and accompanied by authorized personnel at all times?
2. Is written authorization given to those employees who remain in the EFT area after normal working hours? Who gives such authority? Are security guards informed?
3. Are bank terminal operators or others in EFT operations denied access to computer areas or programs?
4. Do procedures prohibit computer personnel from gaining access to bank terminals or test-key information?
5. Does EFT equipment have physical or software locks to prohibit access by unauthorized personnel at all times?
6. Are terminals and other hardware in the EFT area shut down after normal working hours? Are they regulated by automatic time-out controls or time-of-day controls?
7. Are passwords suppressed when they are entered in terminals?
8. Are operator passwords frequently changed? If so, how often?
9. Is supervisory approval required to access terminals at other than authorized times?
10. Are passwords restricted to different levels of access, such as data files and transactions that can be initiated?
11. Are employees prohibited from taking access keys for sensitive equipment or software test keys out of the EFT area?

CONTINGENCY PLANS

1. Has management properly planned for contingencies, and has it developed a reasonable contingency plan and safeguards that are commensurate with the volume of EFT activity?

2. Does the bank maintain backup communications systems, and is supervisory approval required for their use?
3. Are procedures in place for sending and receiving transfers if the bank is forced to operate at a different site?
4. Are backup systems and equipment periodically tested by bank personnel?
5. Are there adequate procedures to ensure that data is recovered by the opening of the next business day's processing?
6. Have written contingency plans been developed and regularly tested in case of partial or complete failure of the bank's systems or of communication lines between the bank and the New York Clearing House, the Federal Reserve Bank, data centers, critical customers, or servicer companies?
7. Are contingency plans reviewed regularly and tested at least annually?
8. Has management distributed contingency plans to all personnel and stored appropriate copies off-site or in a central database?
9. If the bank processes a large volume of payments, does it maintain a backup facility that provides real-time recovery in case of a disaster or other disruption of the primary data center?
10. Are procedures in place for backup, off-site storage of critical information and for inventory control on hardware and software?
11. Do procedures exist to prevent the inadvertent release of test data into the production environment?
12. Are primary and backup telecommunication lines performance-tested frequently by authorized supervisory personnel?

For guidance and listed procedures on Fedline, EFT, and information technology standards, see chapters 18 and 19 of the *FFIEC Information Systems Examination Handbook.*

CONCLUSION

1. Is the foregoing information an adequate basis for evaluating internal control; that is, there are no significant internal-auditing procedures, accounting controls, administrative controls, or other deficiencies or circumstances in areas not covered in this questionnaire that impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
2. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).
3. If intraday credit is granted to any affiliates, has the bank established policies and procedures to monitor and control such exposures and ensure compliance with section 23B of the Federal Reserve Act, as required by Regulation H? (See 12 CFR 250.248.)
4. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (good, medium, or bad).
5. Will the credit risk resulting from funds transfers have an adverse impact on overall asset quality?
6. Does the allowance for loan and lease losses adequately include significant adverse credit risk that is derived from EFT activities?
7. Will the weaknesses identified from the review of payment systems risk and EFT activity have a negative impact on overall liquidity, earnings, or capital?

WHAT'S NEW IN THIS REVISED SECTION

This section was revised to provide additional information about customer identification program (CIP) requirements set forth in Section 326 of the USA PATRIOT Act (referred to as the "CIP" rule). The CIP rule requires a bank to obtain sufficient information to form a reasonable belief regarding the identity of each "customer." The section provides a definition of an "account" and provides information for determining whether an "account" has been created. Under the CIP rule, a person that opens a new account is deemed to be a customer. Refer to SR-16-7 and its interagency attachment.

The role of bank regulators in supervising private-banking activities is (1) to evaluate management's ability to measure and control the risks associated with such activities and (2) to determine if the proper internal control and audit infrastructures are in place to support effective compliance with relevant laws and regulations. In this regard, the supervisors may determine that certain risks have not been identified or adequately managed by the institution, a potentially unsafe and unsound banking practice.

Private-banking functions may be performed in a specific department of a commercial bank, an Edge corporation or its foreign subsidiaries, a nonbank subsidiary, a branch or agency of a foreign banking organization, or multiple areas of an institution. Private banking may also be the sole business of an institution. Regardless of how an institution is organized or where it is located, the results of the private-banking review should be reflected in the entity's overall supervisory assessment.[1]

This section provides examiners with guidance for reviewing private-banking activities at all types and sizes of financial institutions. It is intended to supplement, not replace, existing guidance on the examination of private-banking activities and to broaden the examiner's review of general risk-management policies and practices governing private-banking activities. In addition to providing an overview of private banking, the general types of customers, and the various products and services typically provided, the "Functional Review" subsection describes the critical functions that constitute a private-banking operation and identifies certain safe and sound banking practices. These critical functions are supervision and organization, risk management, fiduciary standards, operational controls, management information systems, audit, and compliance. Included in the risk-management portion is a discussion of the basic "customer-due-diligence" (CDD) principle that is the foundation for the safe and sound operation of a private-banking business. The "Preparation for Examination" subsection assists in defining the examination scope and provides a list of core requests to be made in the first-day letter. Additional examination guidance can be found in this manual, the Federal Financial Institutions Examination Council's (FFIEC) *Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*, the Federal Reserve System's *Trading and Capital-Markets Activities Manual,* and the FFIEC *Information Technology Examination Infobase*.

In reviewing specific functional and product-examination procedures (as found in the private-banking activities module that is part of the framework for risk-focused supervision of large complex institutions), all aspects of the private-banking review should be coordinated with the rest of the examination to eliminate unnecessary duplication of effort. Furthermore, this section has introduced the review of trust activities and fiduciary services, critical components of most private-banking operations, as part of the overall private-banking review. Although the product nature of these activities differs from that of products generated by other banking activities, such as lending and deposit taking, the functional components of private banking (supervision and organization, risk management, operational controls and management information systems, audit, compliance, and financial condition/business profile) should be reviewed across product lines.

Private banking offers the personal and discrete delivery of a wide variety of financial services and products to an affluent market, primarily to high net worth individuals and their corporate interests. A private-banking operation typically offers its customers an all-inclusive

1. Throughout this section, the word *bank* will be used to describe all types of financial institutions, and the term *board of directors* will be interchangeable with *senior management* of branches and agencies of foreign banks.

money-management relationship, including investment portfolio management, financial-planning advice, offshore facilities, custodial services, funds transfer, lending services, overdraft privileges, hold mail, letter-of-credit financing, and bill-paying services. As the affluent market grows, both in the United States and globally, competition to serve it is becoming more intense. Consequently, the private-banking marketplace includes banks, nonbanks, and other types of banking organizations and financial institutions. Private-banking products, services, technologies, and distribution channels are still evolving. A range of private-banking products and services may be offered to customers throughout an institution's global network of affiliated entities—including branches, subsidiaries, and representative offices—in many different regions of the world, including offshore secrecy jurisdictions.

Typically, private-banking customers are high net worth individuals or institutional investors who have minimum investible assets of $1 million or more. Institutions often differentiate domestic from international private banking, and they may further segregate the international function on the basis of the geographic location of their international client base. International private-banking clients may be wealthy individuals who live in politically unstable nations and are seeking a safe haven for their capital. Therefore, obtaining detailed background information and documentation about the international client may be more difficult than it is for the domestic customer. Private-banking accounts may, for example, be opened in the name of an individual, a commercial business, a law firm, an investment adviser, a trust, a personal investment company (PIC), or an offshore mutual fund.

In 2001, the USA PATRIOT Act (the Patriot Act) established new and enhanced measures to prevent, detect, and prosecute money laundering and terrorist financing. In general, these measures were enacted through amendments to the Bank Secrecy Act (BSA). The measures directly affecting banking organizations are implemented primarily through regulations issued by the U.S. Department of the Treasury (31 CFR 1010).[2] Section 326 of the Patriot Act (see the BSA at 31 USC 5318(*l*)) requires financial institutions (such as banks, savings associations, and credit unions) to have customer identification programs.

A customer identification program is dependent on whether an account has been created. An "account" is defined in the CIP rule as "a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account or other extension of credit." An account also includes "a relationship established to provide a safety deposit box or other safekeeping services or to provide cash management, custodian, or trust services."[2a] Under the CIP rule, a person that opens a new account is deemed a customer.[2b] An account *does not include*:

- "products and services for which a formal banking relationship is not generally established with a person, such as check cashing, wire transfer, or the sale of a check or money order" or
- any account that the bank acquires, or accounts opened, to participate in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

(Refer to SR-16-7 and its interagency attachment.) Customer identification programs are to include measures to—

- require that certain information be obtained at account opening (for individuals, the information would generally include their name, address, tax identification number, and date of birth);
- verify the identity of new account holders within a reasonable time period;
- ensure that a banking organization has a reasonable belief that it knows each customer's identity;
- maintain records of the information used to verify a person's identity; and
- compare the names of new customers against government lists of known or suspected terrorists or terrorist organizations.

2. For banking organizations, the regulation implementing the requirements of section 326 of the Patriot Act was jointly issued by the U.S. Department of the Treasury, through the Financial Crimes Enforcement Network (FinCEN), and the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

2a. 31 CFR 1020.100 (a)(1).

2b. 31 CFR 1020.100(c)(1)(i).

A customer identification program is an important component of a financial institution's overall anti-money-laundering and BSA compliance program.

The FFIEC *BSA/AML Examination Manual* provides the interagency BSA examination procedures that should be used to evaluate banking organizations' compliance with the regulation. The examination's scope can be tailored to the reliability of the banking organization's compliance-management system and to the level of risk that the organization assumes. Relevant interagency guidance (in a frequently-asked-question format) has been issued to address the customer identification program rules. (See SR-05-9.)

Private-banking accounts are usually generated on a referral basis. Every client of a private-banking operation is assigned a salesperson or marketer, commonly known as a relationship manager (RM), as the primary point of contact with the institution. The RM is generally charged with understanding and anticipating the needs of his or her wealthy clients and then recommending services and products for them. The number of accounts an RM handles varies, depending on the portfolio size or net worth of the particular accounts. RMs strive to provide a high level of support, service, and investment opportunities to their clients and tend to maintain strong, long-term client relationships. Frequently, RMs take accounts with them to other private-banking institutions if they change employment. Historically, initial and ongoing due diligence of private-banking clients is not always well documented in the institution's files because of RM turnover and confidentiality concerns.

Clients may choose to delegate a great deal of authority and discretion over their financial affairs to RMs. Given the close relationship between clients and their account officers, an integral part of the examination process is assessing the adequacy of managerial oversight of the nature and volume of transactions conducted within the private-banking department or with other departments of the financial institu-

tion, as well as determining the adequacy and integrity of the RM's procedures. Policy guidelines and management supervision should provide parameters for evaluating the appropriateness of all products, especially those involving market risk. Moreover, because of the discretion given to RMs, management should develop effective procedures to review the activity of client accounts in order to protect the client from any unauthorized activity. In addition, ongoing monitoring of account activity should be conducted to detect activity that is inconsistent with the client profile (for example, frequent or sizable unexplained transfers flowing through the account).

Finally, as clients develop a return-on-assets (ROA) outlook to enhance their returns, the use of leveraging and arbitrage is becoming more evident in the private-banking business. Examiners should be alert to the totality of the client relationship product by product, in light of increasing client awareness and use of derivatives, emerging-market products, foreign exchange, and margined accounts.

Products and Services

Personal Investment Companies, Offshore Trusts, and Token-Name Accounts

Private-banking services almost always involve a high level of confidentiality for clients and their account information. Consequently, it is not unusual for private bankers to help their clients achieve their financial-planning, estate-planning, and confidentiality goals through offshore vehicles such as personal investment companies (PICs), trusts, or more-exotic arrangements, such as hedge fund partnerships. While these vehicles may be used for legitimate reasons, without careful scrutiny, they may camouflage illegal activities. Private bankers should be committed to using sound judgment and enforcing prudent banking practices, especially when they are assisting clients in establishing offshore vehicles or token-name accounts.

Through their global network of affiliated entities, private banks often form PICs for their clients. These "shell" companies, which are incorporated in offshore secrecy jurisdictions such as the Cayman Islands, Channel Islands, Bahamas, British Virgin Islands, and Netherlands Antilles, are formed to hold the customer's assets as well as offer confidentiality by opening accounts in the PIC's name. The "beneficial owners" of the shell corporations are typically foreign nationals. The banking institution should know and be able to document that it knows the beneficial owners of such corporations and that it has performed the appropriate due diligence to support these efforts. Emphasis should be placed on verifying the source or origin of the customer's wealth. Similarly, offshore trusts established in these jurisdictions should identify grantors of the trusts and sources of the grantors' wealth. *Anonymous relationships or relationships in which the RM does not know and document the beneficial owner should not be permitted.*

PICs are typically passive personal investment vehicles. However, foreign nationals have established PICs as operating accounts for business entities they control in their home countries. Accordingly, financial institutions should use extra care when dealing with beneficial owners of PICs and associated trusts; these vehicles can be used to conceal illegal activities.

Deposit Taking

A client's private-banking relationship frequently begins with a deposit account and then expands into other products. In fact, many institutions require private-banking customers to establish a deposit account before maintaining any other accounts. Deposit accounts serve as conduits for a client's money flows. To distinguish private-banking accounts from retail accounts, institutions usually require significantly higher minimum account balances and assess higher fees. The private-banking function or institution should have account-opening procedures and documentation requirements that must be fulfilled before a deposit account can be opened. (These standards are described in detail in the "Functional Review" subsection.)

Most private banks offer a broad spectrum of deposit products, including multicurrency deposit accounts that are used by clients who engage in foreign-exchange, securities, and derivatives transactions. The client's transaction activity, such as wire transfers, check writing, and cash deposits and withdrawals, is conducted through deposit accounts (including current accounts). It is very important that the transaction activity into and out of these deposit accounts (including internal transfers between affiliated depository accounts) be closely monitored for suspicious

transactions that are inconsistent with the client's profile of usual transactions. Suspicious transactions could warrant the filing of a Suspicious Activity Report for Depository Institutions (SAR) form. A bank holding company or any nonbank subsidiary thereof, or a foreign bank that is subject to the Bank Holding Company Act (or any nonbank subsidiary of such a foreign bank operating in the United States), is required to file a SAR form in accordance with the provision of section 208.62 of the Federal Reserve Board's Regulation H (12 CFR 208.62) when suspicious transactions or activities are initially discovered and warrant or require reporting. See the expanded procedures for private banking in the FFIEC's *BSA/AML Examination Manual.*

On March 15, 2006, the Board approved a revision to Regulation K (effective April 19, 2006) that incorporates by reference into sections 211.5 and 211.24 of Regulation K section 208.63 of Regulation H. The incorporation results in the requirement that Edge and agreement corporations and other foreign banking organizations (that is, Federal Reserve supervised U.S. branches, agencies, and representative offices of foreign banks) must establish and maintain procedures reasonably designed to ensure and monitor compliance with the BSA and related regulations. Each of these banking organizations' compliance programs must include, at a minimum (1) a system of internal controls to ensure ongoing compliance, (2) independent testing of compliance by the institution's personnel or by an outside party, (3) the designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance, and (4) training for appropriate personnel. (See SR-06-7.)

Investment Management

In private banking, investment management usually consists of two types of accounts: (1) discretionary accounts in which portfolio managers make the investment decisions on the basis of recommendations from the bank's investment research resources and (2) nondiscretionary (investment advisory) accounts in which clients make their own investment decisions when conducting trades. For nondiscretionary clients, the banks typically offer investment recommendations subject to the client's written approval. Discretionary accounts consist of a mixture of instruments bearing varying degrees of market, credit, and liquidity risk that should be appropriate to the client's investment objectives and risk appetite. Both account types are governed under separate agreements between the client and the institution.

Unlike depository accounts, securities and other instruments held in the client's investment accounts are not reflected on the balance sheet of the institution because they belong to the client. These managed assets are usually accounted for on a separate ledger that is segregated according to the customer who owns the assets.

Credit

Private-banking clients may request extensions of credit on either a secured or an unsecured basis. Loans backed by cash collateral or managed assets held by the private-banking function are quite common, especially in international private banking. Private-banking clients may pledge a wide range of their assets, including cash, mortgages, marketable securities, land, or buildings, to securitize their loans. Management should demonstrate an understanding of the purpose of the credit, the source of repayment, the loan tenor, and the collateral used in the financing. When lending to individuals with high net worths, whether on a secured or an unsecured basis, the creditworthiness determination is bolstered by a thorough and well-structured customer-due-diligence process. If that process is not thorough, collateral derived from illicit activities may be subject to government forfeiture.

Borrowing mechanisms are sometimes established to afford nonresident-alien customers the ability to keep financial assets in the United States and to use such assets (via collateralized borrowing arrangements) to provide operating capital for businesses they own and operate in their home countries. Such arrangements enable these customers to keep the existence of the financial assets secret from their home-country authorities and others, while they continue to use the funds (via collateralized borrowings) to fund the businesses at home.

Private bankers need to maintain in the United States adequate CDD information on such nonresident-alien customers and their primary business interests. A well-documented CDD file may include information on the customer from

"who's who" and similar services, Internet research, foreign tax returns and financial statements, checks conducted by the Office of Foreign Assets Control (OFAC), and written and appropriately documented Call Reports prepared by the RM.

While these lending mechanisms may be used for legitimate reasons, management needs to determine whether the arrangements are being used primarily to obfuscate the beneficial ownership of collateral assets, making it difficult for the customer's home-country government to identify who owns the assets. If so, management needs to further determine whether the practice varies from both the appropriate standards of international cooperation for transparency issues and with prudent banking practices, and if so, whether the institution is exposed to elevated legal risk.

Payable-Through Accounts

Another product that may be available in private-banking operations is payable-through accounts (PTAs). PTAs are transaction deposit accounts through which U.S. banking entities ("payable-through banks") extend check-writing privileges to the customers of a foreign bank. The foreign bank ("master account holder") opens a master checking account with the U.S. bank and uses this account to provide its customers with access to the U.S. banking system. The master account is divided into "subaccounts," each in the name of one of the foreign bank's customers. The foreign bank extends signature authority on its master account to its own customers, who may not be known to the U.S. bank. Consequently, the U.S. bank may have customers who have not been subject to the same account-opening requirements imposed on its U.S. account holders. These subaccount customers are able to write checks and make deposits at the U.S. banking entity. The number of subaccounts permitted under this arrangement may be virtually unlimited.

U.S. banking entities engage in PTAs primarily because they attract dollar deposits from the domestic market of their foreign correspondents without changing the primary bank-customer relationship; PTAs also provide substantial fee income. Generally, PTAs at U.S. banking entities have the following characteristics: they are carried on the U.S. banking entity's books as a correspondent bank account, their transaction volume is high, checks passing through the account contain wording similar to "payable through XYZ bank," and the signatures appearing on checks are not those of authorized officers of the foreign bank. See the expanded examination procedures for PTAs in the FFIEC's *BSA/AML Examination Manual.*

Personal Trust and Estates

In trust and estate accounts, an institution offers management services for a client's assets. When dealing with trusts under will, or "testamentary trusts," the institution may receive an estate appointment (executor) and a trustee appointment if the will provided for the trust from the probate. These accounts are fully funded at origination with no opportunity for an outside party to add to the account, and all activities are subject to review by the probate or surrogates' court. On the other hand, with living trusts, or "grantor trusts," the customer (grantor) may continually add to and, in some instances, has control over the corpus of the account. Trusts and estates require experienced attorneys, money managers, and generally well-rounded professionals to set up and maintain the accounts. In certain cases, bankers may need to manage a customer's closely held business or sole proprietorship. In the case of offshore trust facilities, recent changes in U.S. law have imposed additional obligations on those banks that function as trustees or corporate management for offshore trusts and PICs.

A critical element in offering personal trust and estate services is the fiduciary responsibility of the institutions to their customers. This responsibility requires that institutions always act in the best interest of the clients pursuant to the trust documentation, perhaps even to the detriment of the bank. In these accounts, the bank is the fiduciary and the trust officer serves as a representative of the institution. Fiduciaries are held to higher standards of conduct than other bankers. Proper administration of trusts and estates includes strict controls over assets, prudent investment and management of assets, and meticulous recordkeeping. See the expanded examination procedures for trust and asset-management services in the FFIEC's *BSA/AML Examination Manual.*

Custody Services

Custodial services offered to private-banking customers include securities safekeeping, receipt and disbursement of dividends and interest, recordkeeping, and accounting. Custody relationships can be established in many ways, including by referrals from other departments in the bank or from outside investment advisers. The customer or a designated financial adviser retains full control of the investment management of the property subject to the custodianship. Sales and purchases of assets are made by instruction from the customer, and cash disbursements are prearranged or as instructed. Custody accounts involve no investment supervision and no discretion. However, the custodian may be responsible for certain losses if it fails to act properly according to the custody agreement. Therefore, procedures for proper administration should be established and reviewed.

An escrow account is a form of custody account in which the institution agrees to hold cash or securities as a middleman, or a third party. The customer, for example, an attorney or a travel agency, gives the institution funds to hold until the ultimate receiver of the funds "performs" in accordance with the written escrow agreement, at which time the institution releases the funds to the designated party.

Funds Transfer

Funds transfer, another service offered by private-banking functions, may involve the transfer of funds between third parties as part of bill-paying and investment services on the basis of customer instructions. The adequacy of controls over funds-transfer instructions that are initiated electronically or telephonically is extremely important. Funds-transfer requests are quickly processed and, as required by law, funds-transfer personnel may have limited knowledge of the customers or the purpose of the transactions. Therefore, strong controls and adequate supervision over this area are critical. See section 4063.1.

Hold Mail, No Mail, and Electronic-Mail Only

Hold-mail, no-mail, or electronic-mail-only accounts are often provided to private-banking customers who elect to have bank statements and other documents maintained at the institution rather than mailed to their residence. Agreements for hold-mail accounts should be in place, and the agreements should indicate that it was the customer's choice to have the statements retained at the bank and that the customer will pick up his or her mail at least annually. Variations of hold-mail services include delivery of mail to a prearranged location (such as another branch of the bank) by special courier or the bank's pouch system.

Bill-Paying Services

Bill-paying services are often provided to private-banking customers for a fee. If this service is provided, an agreement between the bank and the customer should exist. Typically, a customer may request that the bank debit a deposit account for credit card bills, utilities, rent, mortgage payments, or other monthly consumer charges. In addition, the increased use of the Internet has given rise to the "electronic-mail-only"account, whereby customers elect to have statements, notices, etc., sent to them only by e-mail.

FUNCTIONAL REVIEW

When discussing the functional aspects of a private-banking operation, *functional* refers to managerial processes and procedures, such as reporting lines, quality of supervision (including involvement of the board of directors), information flows, policies and procedures, risk-management policies and methodologies, segregation of duties, management information systems, operational controls (including BSA/AML monitoring), and audit coverage. The examiner should be able to draw sound conclusions about the quality and culture of management and stated private-banking policies after reviewing the functional areas described below. Specifically, the institution's risk-identification process and risk appetite should be carefully defined and assessed. Additionally, the effectiveness of the overall control environment maintained by management should be evaluated by an internal or external audit. The effectiveness of the following functional areas is critical to any private-

banking operation, regardless of its size or product offerings.

Supervision and Organization

As part of the examiner's appraisal of an organization, the quality of supervision of private-banking activities is evaluated. The appraisal of management covers the full range of functions and activities related to the operation of the private bank. The discharge of responsibilities by bank directors should be effected through an organizational plan that accommodates the volume and business services handled, local business practices and the bank's competition, and the growth and development of the institution's private-banking business. Organizational planning is the joint responsibility of senior bank and private-bank management, should be integrated with the long-range plan for the institution, and should be consistent with any enterprise-wide-risk-management program.

Both the directors and management have important roles in formulating policies and establishing programs for private-banking products, operations, internal controls, and audits. However, management alone must implement policies and programs within the organizational framework instituted by the board of directors.

Risk Management

Sound risk-management processes and strong internal controls are critical to safe and sound banking generally and to private-banking activities in particular. Management's role in ensuring the integrity of these processes has become increasingly important as new products and technologies are introduced. Similarly, the client-selection, documentation, approval, and account-monitoring processes should adhere to sound and well-identified practices.

The quality of risk-management practices and internal controls is given significant weight in the evaluation of management and the overall condition of private-banking operations. A bank's failure to establish and maintain a risk-management framework that effectively identifies, measures, monitors, and controls the risks associated with products and services should be considered unsafe and unsound conduct. Furthermore, well-defined management practices should indicate the types of clients that the institution will and will not accept and should establish multiple and segregated levels of authorization for accepting new clients. Institutions that follow sound practices will be better positioned to design and deliver products and services that match their clients' legitimate needs, while reducing the likelihood that unsuitable clients might enter their client account base. Deficiencies noted in this area are weighted in context of the relative risk they pose to the institution and are appropriately reflected in the appraisal of management.

The private-banking function is exposed to a number of risks, including reputational, fiduciary, legal, credit, operational, and market. A brief description of some of the different types of risks follows:

- *Reputational risk* is the potential that negative publicity regarding an institution's business practices and clients, whether true or not, could cause a decline in the customer base, costly litigation, or revenue reductions.
- *Fiduciary risk* refers to the risk of loss due to the institution's failure to exercise loyalty; safeguard assets; and, for trusts, to use assets productively and according to the appropriate standard of care. This risk generally exists in an institution to the extent that it exercises discretion in managing assets on behalf of a customer.
- *Legal risk* arises from the potential of unenforceable contracts, client lawsuits, or adverse judgments to disrupt or otherwise negatively affect the operations or condition of a banking organization. One key dimension of legal risk is supervisory action that could result in costly fines or other punitive measures being levied against an institution for compliance breakdowns.
- *Credit risk* arises from the potential that a borrower or counterparty will fail to perform on an obligation.
- *Operational risk* arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud, or unforeseen catastrophes will result in unexpected losses.

Although effective management of all of the above risks is critical for an institution, certain aspects of reputational, legal, and fiduciary risks are often unique to a private-banking function. In this regard, the following customer-due-

diligence policies and practices are essential in the management of reputational and legal risks in the private-banking functions. (In addition, sound fiduciary practices and conflicts-of-interest issues that a private-banking operation may face in acting as fiduciary are described in the subsection on fiduciary standards.)

Customer-Due-Diligence Policy and Procedures

Sound customer-due-diligence (CDD) policies and procedures are essential to minimize the risks inherent in private banking. The policies and procedures should clearly describe the target client base in terms such as "minimum investable net worth" and "types of products sought," as well as specifically indicate the type of clientele the institution will or will not accept. Policies and procedures should be designed to ensure that effective due diligence is performed on all potential clients, that client files are bolstered with additional CDD information on an ongoing basis, and that activity in client accounts is monitored for transactions that are inconsistent with the client profile and may constitute unlawful activities, such as money laundering. The client's identity, background, and the nature of his or her transactions should be documented and approved by the back office before opening an account or accepting client monies. Certain high-risk clients like foreign politicians or money exchange houses should have additional documentation to mitigate their higher risk.

Money laundering is associated with a broad range of illicit activities: the ultimate intention is to disguise the money's true source—from the initial placement of illegally derived cash proceeds to the layers of financial transactions that disguise the audit trail—and make the funds appear legitimate. Under U.S. money-laundering statutes, a bank employee can be held personally liable if he or she is deemed to engage in "willful blindness." This condition occurs when the employee fails to make reasonable inquiries to satisfy suspicions about client account activities.

Since the key element of an effective CDD policy is a comprehensive knowledge of the client, the bank's policies and procedures should clearly reflect the controls needed to ensure the policy is fully implemented. CDD policies should clearly delineate the accountability and authority for opening accounts and for determining if effective CDD practices have been performed on each client. In addition, policies should delineate documentation standards and accountability for gathering client information from referrals among departments or areas within the institution as well as from accounts brought to the institution by new RMs.

In carrying out prudent CDD practices on potential private-banking customers, management should document efforts to obtain and corroborate critical background information. Private-banking employees abroad often have local contacts who can assist in corroborating information received from the customer. The information listed below should be corroborated by a reliable, independent source, when possible:

- The customer's current address and telephone number for his or her primary residence, which should be corroborated at regular intervals, can be verified through a variety of methods, such as—
  - — visiting the residence, office, factory, or farm (with the RM recording the results of the visit or conversations in a memorandum);
  - — checking the information against the telephone directory; the client's residence, as indicated on his or her national ID card; a mortgage or bank statement or utility or property tax bill; or the electoral or tax rolls;
  - — obtaining a reference from the client's government or known employer or from another bank;
  - — checking with a credit bureau or professional corroboration organization; or
  - — any other method verified by the RM.
- Sufficient business information about the customer should be gathered so that the RM understands the profile of the customer's commercial transactions. This information should include a description of the nature of the customer's business operations or means of generating income, primary trade or business areas, and major clients and their geographic locations, as well as the primary business address and telephone number. These items can be obtained through a combination of any of the following sources:
  - — a visit to the office, factory, or farm
  - — a reliable third party who has a business relationship with the customer
  - — financial statements

  - Dun and Bradstreet reports
  - newspaper or magazine articles
  - LexisNexis reports on the customer or customer's business
  - "Who's Who" reports from the home country
  - private investigations
- Although it is often not possible to get proof of a client's wealth, the RM can use his or her good judgment to derive a reasonable estimate of the individual's net worth.
- As part of the ongoing CDD process, the RM should document in memos or "call reports" the substance of discussions that take place during frequent visits with the client. Additional information about a client's wealth, business, or other interests provides insight into potential marketing opportunities for the RM and the bank, and updates and strengthens the CDD profile.

As a rule, most private banks make it a policy not to accept walk-in clients. If an exception is made, procedures for the necessary documentation and approvals supporting the exception should be in place. Similarly, other exceptions to policy and procedures should readily identify the specific exception and the required due-diligence and approval process for overriding existing procedures.

In most instances, all CDD information and documentation should be maintained and available for examination and inspection at the location where the account is located or where the financial services are rendered. If the bank maintains centralized customer files in locations other than where the account is located or the financial services are rendered, complete customer information, identification, and documentation must be made available at the location where the account is located or where the financial services are rendered within 48 hours of a Federal Reserve examiner's request. Offsite storage of CDD information will be allowed only if the bank has adopted, as part of its customer-due-diligence program, specific procedures designed to ensure that (1) the accounts are subject to ongoing Office of Foreign Assets Control screening that is equivalent to the screening afforded other accounts, (2) the accounts are subject to the same degree of review for suspicious activity, and (3) the bank demonstrates that the appropriate review of the information and documentation is being performed by personnel at the offshore location.

CDD procedures should be no different when the institution deals with a financial adviser or other type of intermediary acting on behalf of a client. To perform its CDD responsibilities when dealing with a financial adviser, the institution should identify the beneficial owner of the account (usually the intermediary's client, but in rare cases, it is the intermediary itself) and perform its CDD analysis with respect to that beneficial owner. The imposition of an intermediary between the institution and counterparty should not lessen the institution's CDD responsibilities.

The purpose of all private-banking relationships should also be readily identified. Incoming customer funds may be used for various purposes, such as establishing deposit accounts, funding investments, or establishing trusts. The bank's CDD procedures should allow for the collection of sufficient information to develop a transaction or client profile for each customer, which will be used in analyzing client transactions. Internal systems should be developed for monitoring and identifying transactions that may be inconsistent with the transaction or client profile for a customer and which may thus constitute suspicious activity.

Suspicious Activity Reports by Depository Institutions. The proper and timely filing of Suspicious Activity Report (SAR) forms is an important component of a bank's CDD program. Since 1996, the federal financial institution supervisory agencies and the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) have required banking organizations to report known or suspected violations of law as well as suspicious transactions on a suspicious activity report or SAR form. See the Board's SAR form regulation (Regulation H, section 208.62 (12 CFR 208.62)).[3] Law enforcement agencies use the information reported on the form to initiate investigations, and Federal Reserve staff use the SAR form information in their examination and oversight of supervised institutions.

A member bank is required to file a SAR form with the appropriate federal law enforcement agencies and the Department of the Treasury. A

3. The Board's SAR form rules apply to state member banks, bank holding companies and their nonbank subsidiaries, some of which have other independent SAR requirements (for example, broker-dealers), Edge and agreement corporations, and the U.S. branches and agencies of foreign banks supervised by the Federal Reserve.

SAR form must be prepared in accordance with the form's instructions and is to be sent to FinCEN when an institution detects—

- insider abuse involving any amount,
- violations aggregating $5,000 or more in which a suspect can be identified,
- violations aggregating $25,000 or more regardless of a potential suspect, or
- transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act.

When a SAR form is filed, the management of a member bank must promptly notify its board of directors or a committee thereof.

A SAR form must be filed within 30 calendar days after the date of initial detection of the facts that may constitute a basis for filing a SAR form. If no suspect was identified on the date of detection of the incident requiring the filing, a member bank may delay filing a SAR form for an additional 30 calendar days in order to identify the suspect. Reporting may not be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. In situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, the financial institution is required to immediately notify an appropriate law enforcement authority in addition to its timely filing of a SAR form.

A bank's internal systems for capturing suspicious activities should provide essential information about the nature and volume of activities passing through customer accounts. Any information suggesting that suspicious activity has occurred should be pursued, and, if an explanation is not forthcoming, the matter should be reported to the bank's management. Examiners should ensure that the bank's approach to SAR forms is proactive and that well-established procedures cover the SAR form process. Accountability should exist within the organization for the analysis and follow-up of internally identified suspicious activity; this analysis should conclude with a decision on the appropriateness of filing a SAR form. See the core procedures concerning suspicious-activity-reporting requirements in the FFIEC *BSA/AML Examination Manual.*

Credit-Underwriting Standards

The underwriting standards for private-banking loans to high net worth individuals should be consistent with prudent lending standards. The same credit policies and procedures that are applicable to any other type of lending arrangement should extend to these loans. At a minimum, sound policies and procedures should address the following: all approved credit products and services offered by the institution, lending limits, acceptable forms of collateral, geographic and other limitations, conditions under which credit is granted, repayment terms, maximum tenor, loan authority, collections and charge-offs, and prohibition against capitalization of interest.

An extension of credit based solely on collateral, even if the collateral is cash, does not ensure repayment. While the collateral enhances the bank's position, it should not substitute for regular credit analyses and prudent lending practices. If collateral is derived from illegal activities, it is subject to forfeiture through the seizure of assets by a government agency. The bank should perform its due diligence by adequately and reasonably ascertaining and documenting that the funds of its private-banking customers were derived from legitimate means. Banks should also verify that the use of the loan proceeds is for legitimate purposes.

In addition, bank policies should explicitly describe the terms under which "margin loans," loans collateralized by securities, are made and should ensure that they conform to applicable regulations. Management should review and approve daily MIS reports. The risk of market deterioration in the value of the underlying collateral may subject the lender to loss if the collateral must be liquidated to repay the loan. In the event of a "margin call," any shortage should be paid for promptly by the customer from other sources pursuant to the terms of the margin agreement.

In addition, policies should address the acceptance of collateral held at another location, such as an affiliated entity, but pledged to the private-banking function. Under these circumstances, management of the private-banking function should, at a minimum, receive frequent reports detailing the collateral type and current valuation. In addition, management of the private-banking function should be informed of any changes or substitutions in collateral.

Fiduciary Standards

Fiduciary risk is managed through the maintenance of an effective and accountable committee structure; retention of technically proficient staff; and development of effective policies, procedures, and controls. In managing its fiduciary risk, the bank must ensure that it carries out the following fiduciary duties:

- *Duty of loyalty.* Trustees are obligated to make all decisions based exclusively on the best interests of trust customers. Except as permitted by law, trustees cannot place themselves in a position in which their interests might conflict with those of the trust beneficiaries.
- *Avoidance of conflicts of interest.* Conflicts of interest arise in any transaction in which the fiduciary simultaneously represents the interests of multiple parties (including its own interests) that may be adverse to one another. Institutions should have detailed policies and procedures regarding potential conflicts of interest. All potential conflicts identified should be brought to the attention of management and the trust committee, with appropriate action taken. Conflicts of interest may arise throughout an institution. Care should be taken by fiduciary business lines, in particular, to manage conflicts of interest between fiduciary business lines and other business lines (including other fiduciary business lines). Consequently, management throughout the institution should receive training in these matters. For more information on the supervision of fiduciary activities, see section 4200.0 in this manual and section 3120.0 of the *Bank Holding Company Supervision Manual.*
- *Duty to prudently manage discretionary trust and agency assets.* Since 1994, the majority of states have adopted laws concerning the prudent investor rule (PIR) with respect to the investment of funds in a fiduciary capacity. PIR is a standard of review that imposes an obligation to prudently manage the portfolio as a whole, focusing on the process of portfolio management, rather than on the outcome of individual investment decisions. Although this rule only governs trusts, the standard is traditionally applied to all accounts for which the institution is managing funds.

Operational Controls

To minimize any operational risks associated with private-banking activities, management is responsible for establishing an effective internal control infrastructure and reliable management information systems. Critical operational controls over any private-banking activity include the establishment of written policies and procedures, segregation of duties, and comprehensive management reporting. Throughout this section, specific guidelines and examination procedures for assessing internal controls over different private-banking activities are provided. Listed below are some of those guidelines that cover specific private-banking services.

Segregation of Duties

Banking organizations should have guidelines on the segregation of employees' duties in order to prevent the unauthorized waiver of documentation requirements, poorly documented referrals, and overlooked suspicious activities. Independent oversight by the back office helps to ensure compliance with account-opening procedures and CDD documentation. Control-conscious institutions may use independent units, such as compliance, risk management, or senior management to fill this function in lieu of the back office. The audit and compliance functions of the private-banking entity should be similarly independent so that they can operate autonomously from line management.

Inactive and Dormant Accounts

Management should be aware that banking laws in most states prohibit banks from offering services that allow deposit accounts to be inactive for prolonged periods of time (generally, 12 or more months with no externally generated account-balance activity). These regulations are based on the presumption that inactive and dormant accounts may be subject to manipulation and abuse by insiders. Policies and procedures should delineate when inactivity occurs and when inactive accounts should be converted to dormant status. Effective controls over dormant accounts should include a specified time between the last customer-originated activity and its classification as dormant, the segregation

of signature cards for dormant accounts, dual control of records, and the blocking of the account so that entries cannot be posted to the account without review by more than one member of senior management.

Pass-Through Accounts and Omnibus Accounts

Pass-through accounts (PTAs) extend checking-account privileges to the customers of a foreign bank; several risks are involved in providing these accounts. In particular, if the U.S. banking entity does not exercise the same due diligence and customer vetting for PTAs as it does for domestic account relationships, the use of PTAs may facilitate unsafe and unsound banking practices or illegal activities, including money laundering. Additionally, if accounts at U.S. banking entities are used for illegal purposes, the entities could be exposed to reputational risk and risk of financial loss as a result of asset seizures and forfeitures brought by law enforcement authorities. It is recommended that U.S. banking entities terminate a payable-through arrangement with a foreign bank in situations in which (1) adequate information about the ultimate users of PTAs cannot be obtained, (2) the foreign bank cannot be relied on to identify and monitor the transactions of its own customers, or (3) the U.S. banking entity is unable to ensure that its payable-through accounts are not being used for money laundering or other illicit purposes.

Omnibus, or general clearing, accounts may also exist in the private-banking system. They may be used to accommodate client funds before an account opening to expedite a new relationship, or they may fund products such as mutual funds in which client deposit accounts may not be required. However, these accounts could circumvent an audit trail of client transactions. Examiners should carefully review a bank's use of such accounts and the adequacy of its controls on their appropriate use. Generally, client monies should flow through client deposit accounts, which should function as the sole conduit and paper trail for client transactions.

Hold-Mail, No Mail, and E-mail-Only Controls

Controls over hold-mail, no-mail, and e-mail-only accounts are critical because the clients have relinquished their ability to detect unauthorized transactions in their accounts in a timely manner. Accounts with high volume or significant losses warrant further inquiry. Hold-mail, no-mail, and e-mail-only account operations should ensure that client accounts are subject to dual control and are reviewed by an independent party.

Funds Transfer—Tracking Transaction Flows

One way that institutions can improve their customer knowledge is by tracking the transaction flows into and out of customer accounts and payable-through subaccounts. Tracking should include funds-transfer activities. Policies and procedures to detect unusual or suspicious activities should identify the types of activities that would prompt staff to investigate the customer's activities and should provide guidance on the appropriate action required for suspicious activity. The following is a checklist to guide bank personnel in identifying some potential abuses:

- indications of frequent overrides of established approval authority or other internal controls
- intentional circumvention of approval authority by splitting transactions
- wire transfers to and from known secrecy jurisdictions
- frequent or large wire transfers for persons who have no account relationship with the bank, or funds being transferred into and out of an omnibus or general clearing account instead of the client's deposit account
- wire transfers involving cash amounts in excess of $10,000
- inadequate control of password access
- customer complaints or frequent error conditions

Custody—Detection of Free Riding

Custody departments should monitor account activity to detect instances of *free-riding,* the

practice of offering the purchase of securities without sufficient capital and then using the proceeds of the sale of the same securities to cover the initial purchase. Free-riding poses significant risk to the institution and typically occurs without the bank's prior knowledge. Free-riding also violates margin rules (Regulations T, U, and X) governing the extension of credit in connection with securities transactions. (See SR-93-13.)

Management Information Systems

Management information systems (MIS) should accumulate, interpret, and communicate information on (1) the private-banking assets under management, (2) profitability, (3) business and transaction activities, and (4) inherent risks. The form and content of MIS for private-banking activities will be a function of the size and complexity of the private-banking organization. Accurate, informative, and timely reports that perform the following functions may be prepared and reviewed by RMs and senior management:

- aggregate the assets under management according to customer, product or service, geographic area, and business unit
- attribute revenue according to customer and product type
- identify customer accounts that are related to or affiliated with one another through common ownership or common control
- identify and aggregate customer accounts by source of referral
- identify beneficial ownership of trust, PIC, and similar accounts

To monitor and report transaction activity and to detect suspicious transactions, management reports may be developed to—

- monitor a specific transaction criterion, such as a minimum dollar amount or volume or activity level;
- monitor a certain type of transaction, such as one with a particular pattern;
- monitor individual customer accounts for variations from established transaction and activity profiles based on what is usual or expected for that customer; and
- monitor specific transactions for BSA compliance.

In addition, reports prepared for private-banking customers should be accurate, timely, and informative. Regular reports and statements prepared for private-banking customers should adequately and accurately describe the application of their funds and should detail all transactions and activity that pertain to the customers' accounts.

Furthermore, MIS and technology play a role in building new and more direct channels of information between the institution and its private-banking customers. Active and sophisticated customers are increasing their demand for data relevant to their investment needs, which is fostering the creation of online information services. Online information can satisfy customers' desire for convenience, real-time access to information, and a seamless delivery of information.

Audit

An effective audit function is vital to ensuring the strength of a private bank's internal controls. As a matter of practice, internal and external auditors should be independently verifying and confirming that the framework of internal controls is being maintained and operated in a manner that adequately addresses the risks associated with the activities of the organization. Critical elements of an effective internal audit function are the strong qualifications and expertise of the internal audit staff and a sound risk-assessment process for determining the scope and frequency of specific audits. The audit process should be risk-focused and should ultimately determine the risk rating of business lines and client CDD procedures. Compliance with CDD policies and procedures and the detailed testing of files for CDD documentation are also key elements of the audit function. Finally, examiners should review and evaluate management's responsiveness to criticisms by the audit function.

Compliance

The responsibility for ensuring effective compliance with relevant laws and regulations may vary among different forms of institutions,

depending on their size, complexity, and availability of resources. Some institutions may have a distinct compliance department with the centralized role of ensuring compliance institution-wide, including private-banking activities. This arrangement is strongly preferable to a situation in which an institution delegates compliance to specific functions, which may result in the management of private-banking operations being responsible for its own internal review. Compliance has a critical role in monitoring private-banking activities; the function should be independent of line management. In addition to ensuring compliance with various laws and regulations such as the Bank Secrecy Act and those promulgated by the Office of Foreign Assets Control, compliance may perform its own internal investigations and due diligence on employees, customers, and third parties with whom the bank has contracted in a consulting or referral capacity and whose behavior, activities, and transactions appear to be unusual or suspicious. Institutions may also find it beneficial for compliance to review and authorize account-opening documentation and CDD adequacy for new accounts. The role of compliance is a control function, but it should not be a substitute for regular and frequent internal audit coverage of the private-banking function. Following is a description of certain regulations that may be monitored by the compliance function.

Office of Foreign Assets Control

The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals. Sanctions are imposed against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under presidential wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and freeze foreign assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments. Under the International Emergency Economic Powers Act, the President can impose sanctions, such as trade embargoes, the freezing of assets, and import surcharges, on certain foreign countries and the "specially designated nationals" of those countries.

A "specially designated national" is a person or entity who acts on behalf of one of the countries under economic sanction by the United States. Dealing with such nationals is prohibited. Moreover, their assets or accounts in the United States are frozen. In certain cases, the Treasury Department can issue a license to a designated national. This license can then be presented by the customer to the institution, allowing the institution to debit his or her account. The license can be either general or specific.

OFAC screening may be difficult when transactions are conducted through PICs, token names, numbered accounts, or other vehicles that shield true identities. Management must ensure that accounts maintained in a name other than that of the beneficial owner are subject to the same level of filtering for OFAC specially designated nationals and blocked foreign countries as other accounts. That is, the OFAC screening process must include the account's beneficial ownership as well as the official account name.

Any violation of regulations implementing designated national sanctions subjects the violator to criminal prosecution, including prison sentences and fines to corporations and individuals, per incident. Any funds frozen because of OFAC orders should be placed in a blocked account. Release of those funds cannot occur without a license from the Treasury Department.

Bank Secrecy Act

Guidelines for compliance with the Bank Secrecy Act (BSA) can be found in the FFIEC *BSA/AML Examination Manual.* See also the question-and-answer format interpretations (SR-05-9) of the U.S. Department of Treasury's regulation (31 CFR 1010) for banking organizations, which is based on section 326 of the Patriot Act. In addition, the procedures for conducting BSA examinations of foreign offices of U.S. banks are detailed in the FFIEC *BSA/AML Examination Manual*. The SAR form filing requirements for nonbank subsidiaries of bank holding companies and state member banks are also set forth in SR-10-8.

PREPARATION FOR EXAMINATION

The following subsections provide examiners with guidance on preparing for the on-site examination of private-banking operations, including determination of the examination scope and drafting of the first-day-letter questionnaire that is provided to the institution.

Preexamination Review

To prepare the examiners for their assignments and to determine the appropriate staffing and scope of the examination, the following guidelines should be followed during the preexamination planning process:

- Review the prior report of examination and workpapers for the exam scope; structure and type of private-banking activities conducted; and findings, conclusions, and recommendations of the prior examination. The prior examination report and examination plan should also provide insight to key contacts at the institution and to the time frame of the prior private-banking review.
- Obtain relevant correspondence sent since the prior examination, such as management's response to the report of examination, any applications submitted to the Federal Reserve, and any supervisory action.
- Research press releases and published news stories about the institution and its private-banking activities.
- Review internal and external audit reports and any internal risk assessments performed by the institution on its private-banking activities. Such reports should include an assessment of the internal controls and risk profile of the private-banking function.
- Contact the institution's management to ascertain what changes have occurred since the last exam or are planned in the near future. For example, examiners should determine if there have been changes to the strategic plan; senior management; or the level and type of private-banking activities, products, and services offered. If there is no mention of private banking in the prior examination report, management should be asked at this time if they have commenced or plan to commence any private-banking activities.
- Follow the core examination procedures in the FFIEC *BSA/AML Examination Manual* in order to establish the base scope for the examination of private-banking activities. Review and follow the expanded procedures for private banking and any other expanded procedures that are deemed necessary.

Examination Staffing and Scope

Once the exam scope has been established and before beginning the new examination, the examiner-in-charge and key administrators of the examination team should meet to discuss the private-banking examination scope, the assignments of the functional areas of private banking, and the supplemental reviews of specific private-banking products and services. If the bank's business lines and services overlap and if its customer base and personnel are shared throughout the organization, examiners may be forced to go beyond a rudimentary review of private-banking operations. They will probably need to focus on the policies, practices, and risks within the different divisions of a particular institution and throughout the institution's global network of affiliated entities.

Reflection of Organizational Structure

The review of private-banking activities should be conducted on the basis of the financial institution's organizational structure. These structures may vary considerably, depending on the size and sophistication of the institution, its country of origin and the other geographic markets in which it competes, and the objectives and strategies of its management and board of directors. To the extent possible, examiners should understand the level of consolidated private-banking activities an institution conducts in the United States and abroad. This broad view is needed to maintain the ''big picture'' impact of private banking for a particular institution.

Risk-Focused Approach

Examiners reviewing the private-banking operations should implement the risk-focused examination approach. The exam scope and

degree of testing of private-banking practices should reflect the degree of risk assumed, prior exam findings on the implementation of policies and procedures, the effectiveness of controls, and an assessment of the adequacy of the internal audit and compliance functions. If initial inquiries into the institution's internal audit and other assessment practices raise doubts about the internal system's effectiveness, expanded analysis and review are required. Examiners should then perform more transaction testing. Examiners will usually need to follow the core examination procedures in the FFIEC *BSA/AML Examination Manual* as well as the expanded procedures for private banking. Other expanded procedures should be followed if circumstances dictate.

First-Day Letter

As part of the examination preparation, examiners should customize the first-day-letter questionnaire to reflect the structure and type of private-banking activities of the institution and the scope of the exam. The following is a list of requests regarding private banking that examiners should consider including in the first-day letter. Responses to these items should be reviewed in conjunction with responses to the BSA, fiduciary, audit, and internal control inquiries:

- organizational chart for the private bank on both a functional and legal-entity basis
- business or strategic plan
- income and expense statements for the prior fiscal year and current year to date, with projections for the remainder of the current and the next fiscal year, and income by product division and marketing region
- balance-sheet and total assets under management (list the most active and profitable accounts by type, customer domicile, and responsible account officer)
- most recent audits for private-banking activities
- copies of audit committee minutes
- copy of the CDD and SAR form policies and procedures
- list of all new business initiatives introduced last year and this year, relevant new-product-approval documentation that addresses the evaluation of the unique characteristics and risk associated with the new activity or product, and an assessment of the risk-management oversight and control infrastructures in place to manage the risks
- list of all accounts in which an intermediary is acting on behalf of clients of the private bank, for example, as financial advisers or money managers
- explanation of the methodology for following up on outstanding account documentation and a sample report
- description of the method for aggregating client holdings and activities across business units throughout the organization
- explanation of how related accounts, such as common control and family link, are identified
- name of a contact person for information on compensation, training, and recruiting programs for relationship managers
- list of all personal investment company accounts
- list of reports that senior management receives regularly on private-banking activities
- description and sample of the management information reports that monitor account activity
- description of how senior management monitors compliance with global policies for worldwide operations, particularly for offices operating in secrecy jurisdictions
- appropriate additional items from the core and expanded procedures for private banking, as set forth in the FFIEC *BSA/AML Examination Manual,* as well as any other items from the expanded procedures that are needed to gauge the adequacy of the BSA/AML program for private-banking activities.

1. To determine if the policies, practices, procedures, and internal controls regarding private-banking activities are adequate for the risks involved.
2. To determine if the bank's officers and employees are operating in conformance with established guidelines for conducting private-banking activities.
3. To assess the financial condition and income-generation results of the private-banking activities.
4. To determine the scope and adequacy of the audit function for private-banking activities.
5. To determine compliance with applicable laws and regulations for private banking.
6. To initiate corrective action when policies, practices, procedures, or internal controls are deficient, or when violations of laws or regulations are found.

As appropriate, the examiner-in-charge should supplement the following procedures with the examination procedures for private banking set forth in the FFIEC's *BSA/AML Examination Manual.* See that manual's core examination procedures for the BSA/AML compliance program and the expanded examination procedures for private banking.

PRIVATE-BANKING PREEXAMINATION PROCEDURES

1. As the examiner-in-charge, conduct a meeting with the lead members of the private-banking examination team and discuss—
   a. the private-banking examination scope (The examination may need to extend beyond a rudimentary review of private-banking operations if the bank's business lines and services overlap and if its customer base and personnel are shared throughout the organization. Examiners will probably need to focus on the policies, practices, and risks within the different divisions of the bank and, if applicable, throughout the bank's domestic or foreign-affiliated entities.);
   b. examiner assignments for the functional areas of private banking; and
   c. the supplemental reviews of specific private-banking products and services.
2. Review the prior report of examination and the previous examination's workpapers; description of the examination scope; structure and type of private-banking activities conducted; and findings, conclusions, and recommendations of the prior examination. The prior examination report and examination plan should also provide information and insight on key contacts at the bank and on the time frame of the prior private-banking review.
3. Review relevant correspondence exchanged since the prior examination, such as management's response to the report of examination, any applications submitted to the Federal Reserve, and any supervisory actions.
4. Research press releases and published news stories about the bank and its private-banking activities.
5. Review internal and external audit reports and any internal risk assessments performed by the bank's internal or external auditors on its private-banking activities. Review information on any assessments of the internal controls and risk profile of the private-banking function.
6. Contact management at the bank to ascertain what changes in private-banking services have occurred since the last examination or if there are any planned in the near future.
   a. Determine if the previous examination or examination report(s) mention private banking; if not, ask management if they have commenced or plan to commence any private-banking activities within any part of the bank's organization.
   b. Determine if there have been any changes to the strategic plan; senior management; or the level and type of private-banking activities, products, and services offered.
   c. During the entire examination of private-banking activities, be alert to the totality of the client relationship, product by product, in light of increasing client awareness and use of derivatives, emerging-market products, foreign exchange, and margined accounts.

FULL-EXAMINATION PHASE

1. After reviewing the private-banking functional areas, draw sound conclusions about the quality and culture of management and stated private-banking policies.
2. Evaluate the adequacy of risk-management policies and practices governing private-banking activities.
3. Assess the organization of the private-banking function and evaluate the quality of management's supervision of private-banking activities. An appraisal of management covers the—
   a. full range of functions (i.e., supervision and organization, risk management, fiduciary standards, operational controls, management information systems, audit, and compliance) and activities related to

the operation of the private-banking activities and

b. discharge of responsibilities by the bank's directors through a long-range organizational plan that accommodates the volume and business services handled, local business practices and the bank's competition, and the growth and development of the bank's private-banking business.

4. Determine if management has effective procedures for conducting ongoing reviews of client-account activity to detect, and protect the client from, any unauthorized activity and any account activity that is inconsistent with the client's profile (for example, frequent or sizable unexplained transfers flowing through the account).
5. Determine if the bank has initiated private-banking account-opening procedures and documentation requirements that must be satisfied before an account can be opened. Determine if the bank maintains internal controls over these procedures and requirements.
6. Determine if the bank requires its subsidiary entities and affiliates to maintain and adhere to well-structured customer-due-diligence (CCD) procedures.
7. Determine if the bank has proper controls and procedures to ensure its proper administration of trust and estates, including strict controls over assets, prudent investment and management of assets, and meticulous recordkeeping. Review previous trust examination reports and consult with the designated Federal Reserve System trust examiners.
8. Ascertain whether the bank adequately supervises its custody services. The bank should ensure that it, and its nonbank entities, have established and currently maintain procedures for the proper administration of custody services, including the regular review of the services on a preset schedule.
9. Determine whether the bank's nonbank subsidiaries and affiliates are required to, and actually maintain, strong controls and supervision over funds transfers.
10. Ascertain if the bank's management and staff are required to perform due diligence, that is, to verify and document that the funds of its private-banking customers were derived through legitimate means, and when extending credit, to verify that the use of loan proceeds was legitimate.
11. Review the bank's use of deposit accounts.
    a. Assess the adequacy of the bank's controls and whether they are appropriately used.
    b. Determine if client monies flow through client deposit accounts and whether the accounts function as the sole conduit and paper trail for client transactions.
12. Determine and ensure that the bank's approach to Suspicious Activity Reports is proactive and that it has well-established procedures covering the SAR process. Establish whether there is accountability within the organization for the analysis and follow-up of internally identified suspicious activity (this analysis includes a sound decision on whether the bank needs to file, or is required by regulation to file, a SAR).

INTRODUCTION

This manual section provides a brief summary of the Board's appraisal regulations and directs readers to the key pieces of guidance that the Board and other banking agencies have issued relating to real estate appraisals and evaluations. The Board's real estate appraisal regulation is found in Regulation Y, subpart G (12 CFR 225.61–67). For state member banks, there is a cross reference to the Board's appraisal regulations in Regulation H (12 CFR 208.50–51). Appraisals are also discussed in the Interagency Guidelines for Real Estate Lending Policies, which are found in Appendix C to Regulation H, (Appendix C to 12 CFR 208). The Board's real estate lending standards (12 CFR 208 Subpart E) direct federally regulated institutions to adopt and maintain written real estate lending policies that are consistent with safe and sound lending practices. Such policies should reflect consideration of applicable regulations and guidance pertaining to real estate appraisals when developing a loan-to-value estimate.[1]

REGULATORY BACKGROUND FOR APPRAISALS

The Board's policy on real estate appraisals emphasizes the importance of sound appraisal policies and collateral-valuation procedures as part of a bank's real estate lending activity. The Board and other federal financial regulatory agencies adopted regulations in August 1990 on the performance and use of appraisals by federally regulated financial institutions to implement statutory changes due to the passage of title XI (title XI) of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) (12 USC 3331 et seq.).[2]

The Board's appraisal regulation requires, at a minimum, that real estate appraisals for federally related transactions be performed in accordance with the Uniform Standards of Professional Appraisal Practice (USPAP) promulgated by the Appraisal Standards Board (ASB) of the Appraisal Foundation, and that appraisals be in writing.[3] The regulation also sets forth additional appraisal standards including that the appraisal contain sufficient information and analysis to support the bank's decision to engage in the transaction, provide the real property's market value, be performed by state certified or licensed appraisers as required by the regulations and analyze deductions and discounts for proposed construction projects, partially leased buildings, nonmarket lease terms, and tract developments with unsold units.

The intent of title XI and the Board's appraisal regulation is to protect federal, financial, and public policy interests in federally related transactions.[4] Federally related transactions are defined as those real estate-related financial transactions that an agency engages in, contracts for, or regulates and that require the services of an appraiser.[5]

Appraisals are required under the appraisal regulation for all real estate-related financial transactions unless an exemption applies. The regulation contains a set of exemptions, including dollar value thresholds at or below which an appraisal is not required. The exemptions are identified as categories of real estate-related financial transactions that do not require the services of an appraiser in order to protect federal financial and public policy interests or to satisfy principles of safe and sound banking. As such, the exempted transactions are not federally related transactions under the statutory and regulatory definitions. Exempted transactions are not subject to title XI nor the provisions of the agencies' regulations governing appraisals. Certain exemptions, however, require the use of an evaluation consistent with safe and sound banking practices. Interagency guidance has been issued to assist financial institutions in performing evaluations consistent with such practices.

In addition to federal regulations, each state has established a program for certifying and licensing real estate appraisers who are qualified to perform appraisals in connection with federally related transactions. Title XI designated the Appraiser Qualifications Board and the ASB of

1. 12 CFR 208, appendix C defines "value" when used to refer to "loan-to-value" as an opinion or estimate set forth in an appraisal or evaluation, whichever may be appropriate, of the market value of real property, prepared in accordance with the agency's appraisal regulations and guidance.

2. In June 1994, the agencies' appraisal regulations were materially revised to clarify, amend, and add several exemptions to the appraisal requirement of regulation.

3. See 12 CFR 225.64.

4. See 12 USC 3331.

5. See 12 USC 3350(4).

the Appraisal Foundation, a nonprofit appraisal industry group, as the authority for establishing qualifications criteria for appraiser certification and licensing and the standards for the preparation of an appraisal. Title XI established the Appraisal Subcommittee (ASC) of the Federal Financial Institutions Examination Council (FFIEC). The ASC monitors state requirements for certifying and licensing appraisers who can perform appraisals for federally related transactions, state supervision, and registration of appraisal management companies, and certain title XI-related requirements established by the federal financial regulatory agencies. The ASC also monitors the Appraisal Foundation and its entities. If the ASC issues a finding that the policies, practices, or procedures of a state appraiser certifying and licensing agency are inconsistent with title XI, the services of licensed or certified appraisers from that state may not be used in connection with federally related transactions. The ASC also maintains the national registry of appraisers and appraisal management companies.[6]

THE APPRAISAL REGULATION

Regulation Y, 12 CFR 225, Subpart G, Appraisal Standards for Federally Related Transactions

The appraisal regulation sets standards for appraisals in connection with federally related transactions and also contains a lists of transactions that do not require the services of an appraiser and, therefore, are exempt from the appraisal requirement of the regulation. In reviewing a real estate loan, examiners assess whether the appraisal supports the real estate value used by the bank in its credit decision and whether the appraisal complies with the appraisal regulation. Further, examiners assess the adequacy of an institution's appraisal program to support its real estate lending activity. There are several key sections in the appraisal regulation, which are described in greater detail below. The regulation contains the following:

- Minimum appraisal standards, Section 225.64
  The regulation establishes minimum standards necessary for all appraisals that are prepared for federally related transactions. Those appraisals must
  - conform to generally accepted appraisal standards in USPAP.
  - be written and contain sufficient information and analysis to support the credit decision.
  - analyze and report deductions and discounts for proposed construction or renovation, partially leased buildings, nonmarket lease terms and tract developments with unsold units.
  - be based upon the definition of market value set forth in the definition section of the regulation.
  - be performed by state-licensed or state-certified appraisers in accordance with the regulation.

- Independence standards for staff appraisers and fee appraisers, Section 225.65
  - Staff appraisers must be independent of the lending, investment, and collection functions of the institution and not involved, except as an appraiser, in the federally related transaction and have no direct or indirect interest, financial or otherwise, in the property.
  - Fee appraisers must be engaged directly by the institution or its agent and have no direct or indirect interest, financial or otherwise, in the property or the transaction.
  - The regulation allows an institution to accept an appraisal prepared by an appraiser engaged by another financial services institution if the appraiser has no direct or indirect interest, financial or otherwise, in the property or transaction, and the appraisal complies with the requirements of the regulation.

- Exemptions from the Regulation, Section 225.63
  - The regulation provides a list of transactions that do not require appraisals. These transactions do not require the services of an appraiser and are, therefore, not federally related transactions. Certain of these

6. Several provisions in title XI of FIRREA were amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act), providing additional authority to the ASC in its oversight of states' appraiser regulatory programs. (See sections 1471-1473 of Pub. L. 111-203, 124 Stat. 1376 (2010).)

exceptions require an evaluation in lieu of an appraisal.

- Standards for professional association membership and competency, Section 225.66
  - A state-certified or state-licensed appraiser may not be excluded from consideration of an assignment based on membership or lack of membership in a particular appraisal organization.
  - All staff and fee appraisers performing appraisals in connection with federally related transactions must be state-certified or state-licensed as appropriate. However any determination of competency shall be based on the individual's experience and educational background as they relate to a particular appraisal assignment.

- Enforcement actions, Section 225.67
  - Institutions and their affiliates, including staff and fee appraisers, may be subject to removal and/or prohibition orders, cease and desist orders, and the imposition of civil money penalties.

SUPERVISORY EXPECTATIONS AND FINDINGS

In conjunction with assessing the overall adequacy of a bank's appraisal and evaluation program to support safe-and-sound real estate lending, examiners may cite a bank with the following possible findings.

1. Examiners may make a finding regarding the bank's compliance with the Board's appraisal regulation. When citing a violation of the appraisal regulation for a state member bank, an examiner should note the matter as a violation of Regulation H (12 CFR 208, subpart E) citing the provision as codified in Regulation Y.
2. In some instances, the finding may indicate that the bank has failed to comply with the Board's real estate lending standards regulation. Examiners may refer to 12 CFR 208, Appendix C, "Interagency Guidelines for Real Estate Lending Policies," for guidance related to the use of appraisals in developing loan-to-value estimates according to the real estate lending standards.
3. Examiners should consider the supervisory expectations in the Interagency Appraisal and Evaluation Guidelines for guidance on safe-and-sound valuation policies and practices. If the institution's valuation policies and practices pose safety and soundness concerns for the institution, examiners could refer to 12 CFR 208, Appendix D-1, "Interagency Guidelines Establishing Standards for Safety and Soundness," for guidance on consideration of the value of underlying collateral.

The following provides examples of possible examination findings and references to the applicable provisions in the Board's regulations.

- Examples of violations of the appraisal regulation, 12 CFR 208.50 as set forth in 12 CFR 225.61–67, include
  - failure to obtain an appraisal (12 CFR 225.63);
    - not obtaining an appraisal as required by the regulation
    - using an outdated appraisal for an existing transaction without meeting the regulatory criteria
    - not obtaining an appraisal due to the misapplication of an exemption, or when the transaction does not meet the specific requirements of the exemption
    - Remedy: Examiners should require the bank to obtain a new appraisal.
  - appraisal fails to comply with the minimum appraisal standards in the appraisal regulation;
    - violation of 12 CFR 208.50, subpart E as set forth in 12 CFR 225.64 (minimum appraisal standards) or 12 CFR 225.65 (appraiser independence)
    - Remedy: Examiners should require the bank to obtain a new appraisal.
  - failure to use a state-licensed or state-certified appraiser (12 CFR 225.63);
    - engaging an appraiser with an expired license or certification
    - engaging a state-licensed appraiser when a state-certified appraiser is required
    - Remedy: Examiners should require the bank to obtain a new appraisal.
  - failure to maintain appraiser independence (12 CFR 225.65); and
    - using a staff appraiser that is not independent of the lending function
    - allowing the borrower to hire the appraiser (the regulation requires that

fee appraisers be engaged directly by the institution or its agent)
  - using an appraisal prepared by an appraiser that has an interest in the real estate
  - Remedy: Examiners should require the bank to obtain a new appraisal.
- failure to obtain an evaluation for certain exempt transactions (12 CFR 225.63(b)).
  - not obtaining an evaluation for a renewed loan
  - not obtaining an evaluation for a commercial or residential transaction at or under the appropriate threshold
  - not obtaining an evaluation for a business loan at or under $1 million
  - For further background, refer to the Interagency Guidelines and the section on "Transactions That Require Evaluations" as well as Appendix A—Appraisal Exemptions.
  - Remedy: Examiners should require the bank to obtain an evaluation.

- Examples of violations of the real estate lending regulation 12 CFR 208, subpart E that pertain to appraisals or evaluations:
  - The bank does not have adequate procedures for monitoring market conditions for its commercial real estate lending.
    - A bank must monitor real estate market conditions in its lending area and have credit administration policies that address the type and frequency of collateral valuations. Violation of 12 CFR 208, subpart E (real estate lending standards regulation).
  - Bank does not have appropriate policies establishing loan-to-value limits for real estate collateral. Violation of 12 CFR 208, subpart E (real estate lending standards regulation).
  - Remedy: Examiners should require the bank to implement policies and procedures to promote compliance with the real estate lending regulation.

- Examples of possible safety and soundness violations:
  - The bank's overall appraisal function is weak.
    - The bank has failed to satisfy supervisory expectations for appraisal and evaluation programs. Guidance on developing appraisal and evaluation programs in a safe-and-sound manner is provided in the Interagency Appraisal and Evaluation Guidelines.
    - The bank's approach to monitoring collateral values raises concerns for the safety and soundness of the institution. For guidance, see in the section of the safety and soundness guidelines, 12 CFR 208, Appendix D-1, which pertains to collateral value.
  - The evaluation is inadequate.
    - The bank has failed to satisfy supervisory expectations for evaluations.
    - For further guidance, refer to the Interagency Guidelines, the "Evaluation Development" and "Evaluation Content" subsections, and Appendix B—Evaluations Based on Analytical Methods or Technological Tools.
    - Remedy: Depending upon the noted deficiencies, examiners should require the bank to perform a new evaluation.
  - The bank has failed to maintain independence expectations for its appraisal and evaluation program. Guidance for doing so is set forth in the section on the Independence of the Appraisal and Evaluation Program in the Interagency Guidelines.
    - Evaluations are prepared by persons who are not independent of loan production.
    - Reporting lines of valuation program staff are not independent of loan production.

INTERAGENCY APPRAISAL AND EVALUATION GUIDELINES

Over the years, the Board and the other federal banking regulatory agencies (the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation (the agencies)) have issued several appraisal-related guidance documents to assist institutions in implementing and complying with the appraisal regulation.[7] In December 2010, the agencies issued the Interagency Appraisal and Evaluation Guidelines (Interagency Guidelines) to clarify their appraisal regulations and to promote best practices in institutions' appraisal and evaluation programs.

7. For more information, see the "Real Estate" supervisory policy and guidance topic page.

(See SR 10-16.) The Interagency Guidelines pertain to all real estate-related financial transactions originated or purchased by a regulated institution or its operating subsidiary for its own portfolio or as assets held for sale, including activities of commercial and residential real estate mortgage operations, capital markets groups, and asset securitization and sales units. The Interagency Guidelines provide a comprehensive discussion of the Board's supervisory expectations for a bank's appraisal and evaluation program as well as background information on the technical aspects of appraisals.

The Interagency Guidelines more fully explain and clarify the requirements of the appraisal regulation. The Interagency Guidelines also contain supervisory guidance for developing and maintaining a safe-and-sound appraisal and evaluation program. Expectations for evaluations are addressed in the guidelines to clarify the requirement in the regulation that evaluations be performed in a safe-and-sound manner. For example, the appraisal regulation allows for the substitution of an "appropriate evaluation" for an appraisal under certain transactions; however, the regulation does not define what is an appropriate evaluation. The Interagency Guidelines provide guidance to assist regulated institutions in determining what an "appropriate evaluation" is. A violation of the appraisal regulation should be cited if the bank failed to obtain an evaluation, where one was required. The Interagency Guidelines may be used as guidance, for example, in determining the appropriate type of content in an evaluation. However, in making determinations about the adequacy of an institution's evaluation content, an assessment of the impact on the safety and soundness of the institution should be made and if it is determined that safety and soundness of the institution was negatively impacted, the safety and soundness guidelines should be cited. The Interagency Guidelines serve two main purposes:

1. Provides guidance regarding supervisory expectations for a bank's appraisal and evaluation program including that
   - the institution's board of directors should provide for an effective appraisal and evaluation program;
   - the program should be independent;
   - the program should have a criteria for selection of appraisers and evaluators;
   - appraisals and evaluations should be appropriately reviewed;
   - there should be appropriate oversight of third party arrangements;
   - the lender should have an appropriate compliance program; and
   - the lender should report appraisers that are involved in USPAP violations to state appraisal regulatory agencies.

2. Clarifies and provides guidance to assist firms in complying with the appraisal regulation, such as
   - the content expectations of an evaluation;
   - independence expectations for evaluations;
   - transactions that are exempt from the appraisal requirement;
   - situations where a real estate loan does not qualify for an exemption;
   - assessing the validity of existing appraisals and evaluations;
   - the importance of a scope of work and valuation approach in appraisal development; and
   - appraisal report options.

The Interagency Guidelines also discuss other uses for appraisals and evaluations. For example, a bank's collateral-valuation program should consider when an appraisal or evaluation should be obtained to monitor ongoing collateral risk and to support credit analysis, including for purposes of updating risk ratings or classifying the credit. Also, when a credit becomes troubled, the primary source of repayment often shifts from the borrower's cash flow and income to the expected proceeds from the sale of the real estate collateral. Therefore, it is important that banks have a sound and independent basis for determining the ongoing value of the real estate collateral. (See SR letter 09-7, "Prudent Commercial Real Estate Loan Workouts.")

Appendixes of Interagency Appraisal and Evaluation Guidelines

Below are summaries of the four appendixes included with the guidelines found in the attachment to SR 10-16.

Appendix A—Appraisal Exemptions. A commentary on the 12 exemptions from the agencies' appraisal regulations. The appendix provides an explanation of the agencies' statutory authority

to provide for appraisal regulatory exemptions and the application of these exemptions.

Appendix B—Evaluations Based on Analytical Methods and Technological Tools. A discussion of the agencies' expectations for evaluations that are based on analytical methods and technological tools, including the use of automated valuation models and tax assessment valuations.

Appendix C—Deductions and Discounts Minimum. A discussion on appraisal standards for determining the market value of a residential tract development, including an explanation of the requirement to analyze and report appropriate deductions and discounts for proposed construction or renovation, partially leased buildings, nonmarket lease terms, and tract developments with unsold units.

Appendix D—Glossary. Definitions of terms related to real estate lending, appraisals, and regulations to aid in reading the guidelines.

ASSESSING THE ADEQUACY OF AN APPRAISAL

When assessing the adequacy of an appraisal and its compliance with the minimum appraisal standards, examiners should assess whether the appraisal conforms to USPAP Standard Rule 1—Real Property Appraisal Development, and USPAP Standard Rule 2—Real Property Appraisal Reporting. The Interagency Guidelines discuss the importance of the appraiser developing an appropriate "scope of work" consistent with USPAP's Scope of Work rule. An appraisal's scope of work should be clearly developed and explained in the appraisal report. Further, the appraisal report should include a copy of the bank's engagement letter with the appraiser for the appraisal assignment.

It is important to note that some of the USPAP standards differ from aspects of the appraisal regulation, and, in such cases, the appraisal regulation should be followed with respect to appraisals for federally related transactions. For example, USPAP does not require appraiser independence and allows for appraisals to address different definitions of value other than market value.

In reviewing a real estate loan and the related appraisal, examiners should consider whether the type of appraisal report is acceptable, the valuation approach is appropriate for the transaction, and the appraisal contains an estimate based on the market value definition. The appraisal should contain a clear development of the market value of the collateral and should contain sufficient information to support the real estate's market value and the bank's credit decision. The USPAP standards discuss all of the basic components of an appraisal. Residential appraisals are commonly completed in a report format that conforms to the Uniform Residential Appraisal Report, which was developed by Fannie Mae and Freddie Mac.

Examiners should also confirm that the bank has procedures for reviewing appraisals and evaluations to determine that an appraisal or evaluation complies with the appraisal regulation and provides sufficient information to support the bank's credit decision. The Interagency Guidelines provide further guidance on appropriate reviews. Not all appraisal reviews need to include the content of a USPAP Standard 3—Appraisal Review, Development, and Reporting. The depth of the appraisal review performed by the bank should consider the complexity and risk of the transaction. If deficiencies are noted in the bank's review process, a bank should obtain a USPAP compliant review completed by an appraiser or obtain a new compliant appraisal. Banks are encouraged to report to the state appraiser regulatory agency any appraiser that violates USPAP standards.

APPRAISAL VALUATION APPROACHES

An appraiser typically utilizes three market-value approaches to analyze the value of property:[8]

- *cost approach*
- *sales comparison approach*
- *income approach*

Appraisers should consider all three approaches to value when completing an appraisal assignment. All three approaches have particular merits depending upon the type of real estate being appraised. For example, for single-family

8. The standards and application of valuation approaches are contained in the USPAP published by the Appraisal Standards Board of the Appraisal Foundation.

residential property, the cost and comparable sales approaches are most frequently used since the common use of the property is the personal residence of the owner. However, if a single-family residential property were intended to be used as a rental property, the appraiser would have to consider the income approach as well. Commercial properties are typically valued using all three approaches to value, however the income approach is heavily favored for property whose primary source of income is derived from rents. The appraiser then correlates the results of the value considerations to determine a market value for the subject real estate. For special-use commercial properties, the appraiser may have difficulty obtaining sales data on comparable properties and may have to base the value estimate on the cost and income approaches.

If an approach is not used in the appraisal, the appraiser should disclose the reason the approach was not used and whether this affects the value estimate.

Cost Approach

The cost approach is commonly used to value construction or improvements to an existing building. In the cost approach to value estimation, the appraiser obtains a preliminary indication of value by adding the estimated depreciated reproduction cost of the improvements to the estimated land value. This approach is based on the assumption that the reproduction cost is the upper limit of value and that a newly constructed building would have functional and mechanical advantages over an existing building. The appraiser would evaluate any functional depreciation (disadvantages or deficiencies) of the existing building in relation to a new structure.

The cost approach consists of four basic steps: (1) estimate the value of the land as though vacant, (2) estimate the current cost of reproducing the existing improvements, (3) estimate depreciation and deduct from the reproduction cost estimate, and (4) add the estimate of land value and the depreciated reproduction cost of improvements to determine the value estimate.

SALES COMPARISON APPROACH

The essence of the sales comparison approach is to determine the price at which similar properties have recently sold on the local market. Through an appropriate adjustment for differences in the subject property and the selected comparable properties, the appraiser estimates the market value of the subject property based on the sales price of the comparable properties. The process used in determining the degree of comparability of two or more properties involves judgment about their similarity with respect to age, location, condition, construction, layout, and equipment. The sales price or list price of those properties deemed most comparable tends to set the range for the value of the subject property.

Income Approach

The income approach estimates the real estate project's expected income over time converted to an estimate of its present value. The income approach is typically used to determine the market value of income-producing properties that receive rent, such as office buildings, apartment complexes, hotels, and shopping centers. In the income approach, the appraiser can apply several different capitalization or discounted cash-flow techniques to arrive at a market value. These techniques include the band-of-investments method, mortgage-equity method, annuity method, and land-residual method. Which method is used depends on whether there is project financing, whether there are long-term leases with fixed-level payments, and whether the value is being rendered for a component of the project, such as land or buildings.

The accuracy of the income-approach method depends on the appraiser's skill in estimating the anticipated future net income of the property and in selecting the appropriate capitalization rate and discounted cash flow. The following data are assembled and analyzed to determine potential net income and value:

- Rent schedules and the percentage of occupancy for the subject property and for comparable properties for the current year and several preceding years. This provides gross rental data and shows the trend of rentals and occupancy, which are then analyzed by the

appraiser to estimate the gross income the property should produce.

- Expense data, such as taxes, insurance, and operating costs paid from revenues derived from the subject property and by comparable properties. Historical trends in these expense items are also determined.
- A time frame for achieving stabilized, or normal, occupancy and rent levels (also referred to as a holding period).

Basically, the income approach converts all expected future net operating income into present-value terms. When market conditions are stable and no unusual patterns of future rents and occupancy rates are expected, the direct capitalization method is used to value income properties. This method calculates the value of a property by dividing an estimate of its stabilized annual income by a factor called a capitalization rate or "cap rate." Stabilized income is generally defined as the yearly net operating income produced by the property at normal occupancy and rental rates; it may be adjusted upward or downward from today's actual market conditions. The cap rate—usually defined for each property type in a market area—is viewed by some analysts as the required rate of return stated as a percentage of current income.

The use of this technique assumes that the use of either the stabilized income or the cap rate accurately captures all relevant characteristics of the property relating to its risk and income potential. If the same risk factors, required rate of return, financing arrangements, and income projections are used, explicit discounting and direct capitalization should yield the same results. For special-use properties, new projects, or troubled properties, the discounted cash flow (net present value) method is the more typical approach to analyzing a property's value. In this method, a time frame for achieving a stabilized, or normal, occupancy and rent level is projected. Each year's net operating income during that period is discounted to arrive at the present value of expected future cash flows. The property's anticipated sales value at the end of the period until stabilization (its terminal or reversion value) is then estimated. The reversion value represents the capitalization of all future income streams of the property after the projected occupancy level is achieved. The terminal or reversion value is then discounted to its present value and added to the discounted income stream to arrive at the total present market value of the property.

Most importantly, the analysis should be based on the ability of the project to generate income over time based upon reasonable and supportable assumptions. Additionally, the discount rate should reflect reasonable expectations about the rate of return that investors require under normal, orderly, and sustainable market conditions.

Value Correlation

The three value estimates—cost, sales comparison, and income—must be evaluated by the appraiser and correlated into a final value estimate based on the appraiser's judgment. Correlation does not imply averaging the value estimates obtained by using the three different approaches. Where these value estimates are relatively close together, correlating them and setting the final market value estimate presents no special problem. It is in situations where widely divergent values are obtained by using the three appraisal approaches that the examiner must exercise judgment in analyzing the results and determining the estimate of market value.

Other Definitions of Value

While the Board's appraisal regulation requires that the appraisal contain the market value of the real estate collateral, there are other definitions of value that are encountered in appraising and evaluating real estate transactions. These include the following:

Fair value. This is an accounting term that is generally defined as the amount in cash or cash-equivalent value of other consideration that a real estate parcel would yield in a current sale between a willing buyer and a willing seller (the selling price), that is, other than in a forced or liquidation sale.[9] According to accounting litera-

9. See Accounting Standards Codification (ASC) Topic 820, "Fair Value Measurements and Disclosures" (formerly FASB Statement No. 157, "Fair Value Measurements"). It defines fair value and establishes a framework for measuring fair value. ASC Topic 820 should be applied when other accounting topics require or permit fair value measurements. Fair value is defined as the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants in the asset's or liability's principal (or most advantageous) market at the measurement date. This value is often referred to as an "exit" price. An orderly

ture, fair value is generally used in valuing assets in nonmonetary transactions, troubled debt restructuring, quasi-reorganizations, and business combinations accounted for by the purchase method. An accountant generally defines fair value as market value; however, depending on the circumstances, these values may not be the same for a particular property.

Investment value. This is based on the data and assumptions that meet the criteria and objectives of a particular investor for a specific property or project. The investor's criteria and objectives are often substantially different from participants' criteria and objectives in a broader market. Thus, investment value can be significantly higher than market value in certain circumstances and should not be used in credit analysis decisions.

Liquidation value. This assumes that there is little or no current demand for the property but the property needs to be disposed of quickly, resulting in the owner sacrificing potential property appreciation for an immediate sale.

transaction is a transaction that assumes exposure to the market for a period prior to the measurement date to allow for marketing activities that are usual and customary for transactions involving such assets or liabilities; it is not a forced liquidation or distressed sale.

Going-concern value. This is based on the value of a business entity rather than the value of just the real estate. The valuation is based on the existing operations of the business that has a proven operating record, with the assumption that the business will continue to operate.

Tax-assessed value. This represents the value on which a taxing authority bases its assessment. The assessed value and market value may differ considerably due to tax assessment laws, timing of reassessments, and tax exemptions allowed on properties or portions of a property.

Net realizable value (NRV). This is recognized under generally accepted accounting principles as the estimated selling price in the ordinary course of business less estimated costs of completion (to the stage of completion assumed in determining the selling price), holding, and disposal. The NRV is generally used to evaluate the carrying amount of assets being held for disposition and properties representing collateral. While the market value or future selling price are generally used as the basis for the NRV calculation, the NRV also reflects the current owner's costs to complete the project and to hold and dispose of the property. For this reason, the NRV will generally be less than the market value.

1. Is the appraisal and evaluation program adequate for the size, complexity, and nature of the bank's real estate related activities?
2. Is the appraisal and evaluation program independent from the loan production process?
3. Do the bank's policies ensure that appraisals and evaluations meet minimum standards?
4. Does the bank have appropriate procedures for updating appraisals as needed?
5. Does the bank have an appropriate appraisal review program?
6. Does the bank take appropriate actions to ensure compliance with the appraisal program expectations?
7. Does the bank appropriately oversee third parties involved in the appraisal process?
8. Does the bank have policies and procedures to ensure the independence of staff and fee appraisers?
9. Does the bank have policies to ensure that appraisers meet licensing and competency standards?

PRELIMINARY REVIEW

1. Review the following documents:

   - Prior examination reports, prior examination work papers, pre-examination memorandum, and file correspondence (for an overview of previously identified program deficiencies, violations, and concerns);
   - Internal and external loan reviews (look for individual real estate appraisal issues);
   - Appraisal and evaluation policies and procedures;
   - Internal and external reviews of the adequacy of the real estate appraisal and evaluation program;
   - List of board-approved appraisers;
   - Log of all appraisal engagements for each appraiser for the current and prior year; and
   - Organizational charts and reporting structures with respect to the institution's appraisal and evaluation program. (Note: Review the institution's organizational structure to understand better whether its program is isolated from influence by the loan production staff or if mitigating controls are in place for institutions with a small staff size.)

SUPERVISORY POLICY

2. Determine whether the institution's appraisal and evaluation program is adequate for the size, complexity, and nature of its real estate related activities.

APPRAISAL AND EVALUATION PROGRAM

3. Determine whether the institution's board of directors established policies and procedures to review and revise its program as necessary.

INDEPENDENCE OF THE APPRAISAL AND EVALUATION PROGRAM

4. Determine whether the institution's appraisal and evaluation program is independent from loan production and collection. Consider whether policies and procedures address the following:

   - Individuals providing evaluation services should be prohibited from having an interest, financial or otherwise, in the property or the transaction.
   - Reporting lines for staff who administer the appraisal and evaluation program (including the ordering, reviewing, and acceptance of appraisals and evaluations) should be independent of loan production.
   - Management should establish safeguards (if absolute lines of independence cannot be achieved) to isolate its program from influence from the loan production process and to ensure that any person who ordered or reviewed the appraisal or evaluation abstains from decisions on loan approvals.

SELECTION OF APPRAISERS OR PERSONS WHO PERFORM EVALUATIONS

5. Determine whether the appraisal and evaluation program has criteria for selecting, evaluating, and monitoring the performance of appraisers and persons who perform evaluations. Determine whether policies and procedures appropriately address

   - the documented assessment of whether the appraiser or person performing an evaluation is competent, independent, and has adequate experience and knowledge of the market, location, and type of property being valued;
   - the development and administration of the approved appraiser list that include a process for
     — qualifying an appraiser for initial placement on the list, and

— monitoring the appraiser's performance and credentials to assess whether to retain the appraiser on the list;
- safeguards for developing and administering the approved appraiser list independent of the loan production process;
- the use of written engagement letters when ordering appraisals, particularly for large, complex, or out-of-area commercial real estate properties; and
- the acceptance of appraisal reports performed for another financial institution.

TRANSACTIONS THAT REQUIRE APPRAISALS

6. Determine whether an appraisal or evaluation that supports the lending decision, or an explanation why a new appraisal or evaluation was not required, is contained in the credit files or is available.

MINIMUM APPRAISAL STANDARDS

7. Determine whether the institution has procedures and internal controls that ensure appraisals for federally related transactions

   - conform to generally accepted appraisal standards as evidenced by the USPAP promulgated by the Appraisal Standards Board of the Appraisal Foundation;
   - contain sufficient information and analysis to support the institution's decision to engage in the transaction;
   - analyze and report appropriate deductions and discounts for proposed construction or renovation, partially leased buildings, nonmarket lease terms, and tract developments with unsold units;
   - use definitions of market value set forth in the appraisal regulation; and
   - are performed by state-licensed or state-certified appraisers in accordance with the requirements set forth in the appraisal regulation.

8. Determine whether the program prohibits the use of a broker price opinion in connection with consumer transactions.

APPRAISAL DEVELOPMENT

9. Determine whether the institution considers the risk, size, and complexity of the transaction and real estate collateral when analyzing an appraisal. Consider whether policies and procedures ensure appraisals have an appropriate scope that provides for credible assignment results. Appraisals should reflect

   - the extent to which the property is identified and inspected,
   - the type and extent of data researched, and
   - the analyses applied to arrive at opinions or conclusions.

APPRAISAL REPORTS

10. Determine whether the institution considers the risk, size, and complexity of the transaction and the real estate collateral when requesting the appraisal report format. Appraisal reports should contain sufficient information and analysis to support the institution's decision to engage in the transaction.

TRANSACTIONS THAT REQUIRE EVALUATIONS

11. Determine whether the institution established criteria for when the appraisal regulations permit the use of an evaluation in lieu of an appraisal for transactions that qualify for certain exemptions.

    - Although appraisal regulations permit the use of evaluations for certain transactions, ensure the institution has policies and procedures for determining when to obtain an appraisal for high-risk transactions.

EVALUATION DEVELOPMENT

12. Determine whether evaluations provide credible estimates of collateral market values as of a specific date and are completed prior to the decision to enter into a transaction. Consider

- the institution's documentation requirements for ensuring the sufficiency of information and analysis to support the estimate of value for a given transaction.
- the institution's criteria for determining the level and extent of research or inspection necessary to ascertain the property's physical condition and the economic and market factors that should be considered in developing an evaluation.

EVALUATION CONTENT

13. Consider whether evaluations

- identify the location of the property;
- provide a description of the property and its current and projected use;
- provide an estimate of the property's market value in its actual physical condition, use, and zoning designation as of the effective date of the evaluation, with any limiting conditions;
- describe the method(s) the institution used to confirm the property's actual physical condition and the extent to which an inspection was performed;
- describe the analysis that was performed and the supporting information that was used in valuing the property;
- describe the supplemental information that was considered when using an analytical method or technological tool;
- indicate all source(s) of information used in the analysis, as applicable, to value the property; and
- include information on the preparer when an evaluation is performed by a person, such as the name and contact information, and signature (electronic or other legally permissible signature) of the preparer.

VALIDITY OF APPRAISALS AND EVALUATIONS

14. Determine whether the program establishes criteria for assessing whether existing appraisals or evaluations continue to reflect current market values.

- Documentation in the credit files should provide the facts and analysis to support the institution's conclusion that the existing appraisal or evaluation may be used in a subsequent transaction.
- Criteria should be in place for obtaining a new appraisal or evaluation when an existing appraisal or evaluation is no longer valid for a subsequent transaction.

REVIEWING APPRAISALS AND EVALUATIONS

15. Determine whether an institution's policies and procedures for reviewing appraisals and evaluations

- require the receipt and review of appraisal reports and evaluations prior to making the final credit decision;
- address the independence, education, training and qualifications, and role of the reviewer;
- reflect a risk-focused approach for determining the depth of the review;
- establish a process for resolving any deficiencies in appraisals or evaluations; and
- set forth documentation standards for the review and the resolution of noted deficiencies.

THIRD-PARTY ARRANGEMENTS

16. Determine whether the institution has adequate procedures governing the selection, use, and oversight of a third party that performs appraisal management services. Consider the following:

- procedures for governing the due diligence for selecting and entering into an arrangement with a third party;
- internal controls for identifying, monitoring, and managing the risks associated with using a third party arrangement for valuation services;
- documentation of the results of monitoring and periodic assessments of the third party's compliance with applicable regulations and consistency with supervisory guidance;
- timeliness of remedial actions taken when deficiencies are discovered;
- the institution's requirements for the third

party to select a competent, qualified, and independent individual or appraiser to perform an evaluation;
- the institution's requirements for the third party to select a state-licensed or state-certified appraiser for a given appraisal; and
- the institution's requirements for the third party to notify the appraiser or the person who performs the evaluation that the institution is the client.

PROGRAM COMPLIANCE

17. Determine whether the institution's appraisal and evaluation policies establish internal controls to promote an effective appraisal and evaluation program. Consider the following:
    - policies and procedures address the need for obtaining current collateral valuation information for monitoring the collateral position over the life of a credit and managing the risk in the real estate credit portfolios;
    - criteria for determining when to obtain a new appraisal or evaluation when there is deterioration in the credit since origination or changes in market conditions;
    - current collateral valuation information to assess collateral risk and facilitate an informed decision on whether to engage in a modification or workout of an existing real estate credit;
    - periodic and independent review of the institution's appraisal and evaluation program and its corresponding internal controls; and
    - procedures to ensure appraisers receive a customary and reasonable fee when the assignment is for a transaction secured by a consumer's principal dwelling, as required by 12 CFR 1026.42.

18. Determine whether management takes action to correct prior deficiencies noted in examination, audit, and loan review reports.

19. Determine whether there is a significant correlation between classified assets and unsubstantiated appraisals and evaluations.

REFERRALS

20. Determine whether the institution has policies, procedures, and internal controls governing the filing of complaints with the appropriate state appraiser regulatory agency or suspicious activity reports (SARs) with the Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury. Consider the following:
    - Complaints are filed with the appropriate state appraiser regulatory officials when it suspected that a state-certified or state-licensed appraiser failed to comply with USPAP, applicable state laws, or engaged in other unethical or unprofessional conduct; and
    - SARs are filed with FinCEN when suspecting fraud or identifying other transactions meeting the SAR filing criteria.

AUTOMATED VALUATION MODELS (COMPLETE IF THE BANK USES AN AUTOMATED VALUATION MODEL)

21. Evaluate the institution's policies, procedures, and internal controls governing the selection, use, and validation of the valuation method or tool used in the development of an evaluation. Determine whether policies and procedures governing the selection of automated valuation models (AVM) include
    - performing an adequate level of due diligence in selecting an AVM vendor and its models, considering how model developers conducted performance testing as well as the sample size used and the geographic level tested (such as county level or zip code);
    - establishing an acceptable minimum performance criteria for a model prior to and independent of the validation process;
    - validating the model(s) during the selection process and documentation of the validation process;
    - evaluating the underlying data used in the model(s), including the data sources and types, frequency of updates, quality control performed on the data, and the sources

of the data in states where public real estate sales data are not disclosed;
- assessing modeling techniques and the inherent strengths and weaknesses of different model types as well as how a model(s) performs for different property types; and
- evaluating the AVM vendor's scoring system and methodology for the model(s), including a determination that the scoring system provides an appropriate indicator of model reliability by property type and geographic location.

22. Evaluate management's implementation and oversight of AVMs. Consider the following:

    - procedures for monitoring the use of an AVM(s), including an ongoing validation process;
    - established AVM performance criteria for accuracy and reliability in a given transaction, lending activity, and geographic location;
    - established criteria for deciding whether a particular valuation method or tool is appropriate for a given transaction or lending activity, considering associated risks, including transaction size and purpose, credit quality, and leverage tolerance (loan-to-value);
    - appropriate controls to ensure that the selected method or tool produce a reliable estimate of market value that supports its decision to engage in a transaction;
    - established criteria to determine when market events or risk factors would preclude the use of a particular method or tool;
    - policies governing the use of multiple methods or tools, if applicable, for valuing the same property or to support a particular lending activity;
    - internal controls to preclude *value shopping* when more than one AVM is used for the same property; and
    - policies and procedures that address the extent to which an inspection or research should be performed to ascertain the property's actual physical condition, and supplemental information should be obtained to assess the effect of market conditions or other factors on the estimate of market value.

SAMPLE TESTING

23. Determine whether the institution's program ensures that appraisals for federally related transactions

    - disclose the purpose and use of the appraisal;
    - provide an opinion of the collateral's market value as defined in the appraisal regulation and clarified in supervisory guidance;
    - provide an effective date for the opinion of market value;
    - provide the sales history of the subject property for the prior three years;
    - provide the valuation approaches (that is cost, income, and sales comparison approaches) that are applicable for the property type and market;
    - include an analysis and reporting of appropriate deductions and discounts when the appraisal provides a market value estimate based on the future demand of the real estate (such as proposed construction, partially leased buildings, nonmarket lease terms, and unsold units in a residential tract development);
    - evaluate and reconcile the valuation approaches into an opinion of market value estimate based on the appraiser's judgment, if multiple approaches were used;
    - explain why a valuation approach is inappropriate and not used in the appraisal;
    - support the assumptions and the value conclusion rendered through adequate documentation and information on market conditions and trends;
    - evaluate key assumptions and potential ramifications to the opinion of market value if these assumptions are not realized;
    - present an opinion of the real property's market value in an appraisal report
    - option that addresses the property's type, market, and risk and type of transaction;
    - provide a level of detail in the appraisal report sufficient to explain and support the appraiser's opinion of market value; and
    - disclose and define other value opinions (such as disposal value of the property or the value of non-real property), if the institution requests such information.

24. Verify that the

    - institution selects appraisers who are qualified, independent, and appropriately state-licensed or certified; and
    - appraiser's expertise and qualifications demonstrate that the appraiser was competent for the market and property type.

25. Determine the following for appraisals that include the cost approach to value:

    - The values for land and improvements are presented separately,
    - Cost estimates appear to be reasonable,
    - The value allocated to land component of the property is supported by comparable land sales, and
    - Estimates for depreciation appear reasonable and consistent with estimates of effective age of the improvement.

26. Determine the following for appraisals that include the income approach to value:

    - Potential income projections appear reasonable;
    - Adjustments for vacancy and credit loss appear adequate;
    - Operating expenses appear reasonable;
    - Capitalization rates appear reasonable and are supported by market data;
    - Terms and conditions of existing leases reflect market;
    - For an income-producing property subject to existing leases, the value reflects the value of leased fee estate; and
    - For a property to be developed or constructed, assumptions on the construction period, time frame for achieving stabilized occupancy, and expectations for sales absorption rate or lease-up period are reasonable and reflective of market conditions.

27. Determine the following for appraisals that include the sales comparison approach to value:

    - Comparable properties are physically similar;
    - Comparable properties are economically similar;
    - Comparable sales are sufficiently recent (that is, substantial changes in the market have not occurred since the time of the comparable sale); and
    - Adjustments to comparable values are made for any sales concessions, including favorable financing or seller concessions that are not typical in the market.

28. Determine the following for a residential tract development (five or more residential units in the same development):

    - The appraisal includes a market value of the property that reflects deductions and discounts for holding costs, marketing costs, and entrepreneurial profit supported by market data.

Review the bank's internal controls, policies, practices, and procedures for real estate appraisals and evaluations. The bank's system should be accurately and fully documented and should include, where appropriate, narrative descriptions, flow charts, copies of forms used, and other pertinent information. Items marked with an asterisk require substantiation by observation or testing.

POLICIES

1. Has the board of directors, consistent with its duties and responsibilities, adopted written appraisal and evaluation policies that define the following:
   a. bank management's responsibility for selecting, evaluating, monitoring, and ensuring the independence of the individual who is performing the appraisal or evaluation?
   b. the basis for selecting staff appraisers and engaging fee appraisers for a particular appraisal assignment and for ensuring that the individual is independent of the transaction; possesses the requisite qualifications, expertise, and educational background; demonstrates competency for the market and property type; and has the required state certification or license if applicable?
   c. procedures for when to obtain appraisals and evaluations?
   d. procedures for prohibiting the use of a borrower-ordered or borrower-provided appraisal?
   e. procedures for monitoring collateral risk on a loan and portfolio basis as to when to obtain a new appraisal or new evaluation, including the frequency, triggering events, scope of appraisal work, valuation methods, and report option?
   f. appraisal and evaluation compliance procedures to determine that appraisals and evaluations are reviewed by qualified and adequately trained individuals who are not involved in the loan-production process?
   g. appraisal and evaluation review procedures to ensure that the bank's appraisals and evaluations are consistent with the standards of USPAP and the Board's regulation and guidelines?
   h. appraisal and evaluation review procedures that require the performance of the review prior to the credit decision, resolution of noted deficiencies, and documentation of the review in the credit file, and, if necessary, obtaining a second appraisal or relying on USPAP's Standard Rule 3 in performing a review or performing another evaluation?
   i. an appropriate level of review for appraisals and evaluations ordered by the bank's agents or obtained from another financial services institution?
   j. adequate level of oversight when the bank uses a third party for appraisal management services?
   k. use of analytical methods and technological tools (such as automated valuation models or tax assessment valuations) in the development of evaluations that is appropriate for the risk and type of transaction and property?
   l. internal controls to prevent officers, loan officers, or directors who order or review appraisals and evaluations from having the sole authority for approving the requested loans?
   m. procedures for promoting compliance with the appraisal independence provisions of Regulation Z (Truth in Lending) for open- and closed-end consumer credit transactions secured by a consumer's principal dwelling?
2. Does the board of directors annually review these policies and procedures to ensure that the appraisal and evaluation policies and procedures meet the needs of the bank's real estate lending activity and remains compliant with the Board's regulation and supervisory guidance?

APPRAISALS

*1. Are appraisals in writing, dated, and signed by the appraiser?
*2. Does the appraisal meet the minimum standards of the Board's regulation and USPAP, and contain sufficient information and analysis to support the bank's decision

to engage in the transaction? Does the appraisal

a. reflect an appropriate scope of work that will provide for credible results, including the extent to which the property is identified and inspected, the type and extent of data research performed, and the analyses applied to arrive at an opinion of market value?
b. disclose the purpose and use of the appraisal?
c. provide an opinion of the collateral market value as defined in the Board's appraisal regulation and further clarified in supervisory guidance?
d. provide an effective date for the opinion of market value?
e. provide the sales history of the subject property for the prior three years?
f. reflect valuation approaches (that is, cost, income, and sales comparison approaches) that are applicable for the property type and market?
g. include an analysis and reporting of appropriate deductions and discounts when the appraisal provides a market value estimate based on the future demand of the real estate (such as proposed construction, partially leased buildings, nonmarket lease terms, and unsold units in a residential tract development)?
h. evaluate and reconcile the three approaches into an opinion of market value estimate based on the appraiser's judgment?
i. explain why an approach is inappropriate and not used in the appraisal?
j. fully support the assumptions and the value rendered through adequate documentation and information on market conditions and trends?
k. evaluate key assumptions and potential ramifications to the opinion of market value if these assumptions are not realized?
l. present an opinion of the collateral's market value in an appraisal report option that addresses the property type, market, risk, and type of transaction?
m. disclose and define other value opinions (such as disposal value of the property or the value of non-real property), if the bank requests such information?

*3. Are appraisals received before the bank makes its final credit or other credit decision or was the loan granted a conditional approval? When loans have conditional approvals pending receipt of an appraisal, confirm that appraisals are received, reviewed, and accepted for the transaction.

*4. If the bank is depending on an appraisal obtained for another financial services institution as support for its transaction, does the bank have appraisal review procedures to ensure that the appraisal meets the standards of the appraisal regulation, including independence? (These types of transactions would include loan participations, loan purchases, and mortgage-backed securities.)

*5. If an appraisal for one transaction is used for a subsequent transaction, does the bank sufficiently document its determination that the appraiser is independent, the appraisal complies with the appraisal regulations, and the appraisal is still valid?

APPRAISERS

1. Are appraisers fairly considered for assignments regardless of their membership or lack of membership in a particular appraisal organization?
2. Before the bank selects an appraiser for an assignment, does the bank confirm that the appraiser has the requisite qualifications, education, experience, and competency for both the property type and market to complete the appraisal?
3. If a bank pre-screens appraisers and uses an approved appraiser list, does the bank have procedures for assessing an appraiser's qualifications, selecting an appraiser for a particular assignment, and evaluating the appraiser's work for retention on the list?
4. The following items apply for large, complex, or out-of-area commercial real estate properties:
   a. Are written engagement letters used when ordering appraisals, and are copies of the letters retained or included in the appraisal report?
   b. Does the bank have procedures for resolving deficiencies in appraisals, including determining when such appraisals should be reviewed by another

appraiser (that is, a USPAP Standard Rule 3—Appraisal Review)?

5. Are appraisers independent of the transaction?
   a. Are staff appraisers independent of the lending, investment, and collection functions and not involved, except as an appraiser, in the federally related transaction? Has a determination been made that they have no direct or indirect interest, financial or otherwise, in the property?
   b. Are fee appraisers engaged directly by the bank or its agent? Has a determination been made that they have no direct or indirect interest, financial or otherwise, in the property or transaction?
   c. Are any appraisers recommended or selected by the borrower (applicant)?
6. If the bank has staff appraisers to perform appraisals or appraisal reviews, does the bank periodically have independent appraisers evaluate their work for quality and confirm that they have the knowledge and competency to perform their work and continue to hold the appropriate state license or certification?
7. If fee appraisers are used by the bank, does the bank investigate their qualifications, experience, education, background, and reputations?
8. Is the status of an appraiser's state certification or license verified with the state appraiser regulatory authority to ensure that the appraiser is in good standing?
9. Does the bank have procedures for filing complaints with the appropriate state appraiser regulatory officials when it suspects the fee appraiser failed to comply with USPAP, applicable state laws, or engaged in other unethical or unprofessional conduct?
10. Are fee appraisers paid the same fee whether or not the loan is granted?
11. Does the bank pay a customary and reasonable fee for appraisal services in the market where the property is located when the appraisal is for an open- and closed-end consumer credit transaction secured by a consumer's principal dwelling as required under Regulation Z?

EVALUATIONS

1. Are the individuals performing evaluations independent of the transaction?

*2. Are the evaluations required to be in writing, dated, and signed?

*3. Does the bank require sufficient information and documentation to support the estimate of value and the individual's analysis?

*4. Are the development and content of the evaluation reflective of transaction risk and appropriate for the property type?

*5. Are the valuation methods used, and does the supporting information in the evaluation provide a reliable estimate of the property's market value as of a stated effective date prior to the credit decision?

*6. If analytical methods or technological tools are used in the development of an evaluation, is the use of the method or tool consistent with safe and sound banking practices?

*7. If an evaluation obtained for one transaction is used for a subsequent transaction, does the bank sufficiently document its determination that the evaluation is still valid?

*8. Are evaluations received before the bank enters into a loan commitment?

*9. Does the bank have evaluation review procedures to ensure that the evaluation meets safe-and-sound banking practices?

*10. If a tax assessment valuation is used in the development of an evaluation, has the bank demonstrated that there is a valid correlation between the tax assessment data and the property's market value?

EVALUATORS

1. Are individuals who perform evaluations competent to complete the assignment?
2. Do the individuals who perform evaluations possess the appropriate collateral valuation training, expertise, and experience relevant to the type of property being valued?
3. Are evaluations prepared by individuals who are independent of the transaction?

MONITORING COLLATERAL VALUES

1. Does the bank have policies to monitor collateral risk on a portfolio and on an individual credit basis?
2. Does the policy address the need to obtain current valuation information for collateral supporting an existing credit that may be modified or considered for a loan workout?
3. Does the criteria for determining when to obtain a new appraisal or new evaluation address deterioration in the credit; material changes in market conditions; and revisions to, or delays in, the project's development and construction?
4. Does the bank sufficiently document and follow its criteria for obtaining reappraisals or reevaluations?

THIRD-PARTY ARRANGEMENTS

1. Did the bank exercise appropriate due diligence in the selection of a third party to perform appraisal management services for the bank?
2. Does the bank have the resources and expertise necessary for performing ongoing oversight of such third party arrangements?
3. Does the bank have the internal controls for identifying, monitoring, and managing the risks associated with the use of the third party?
4. Does the bank adequately document the results of its ongoing monitoring and periodic assessments of the third party's compliance with applicable regulations and with supervisory expectations?
5. Does the bank take timely remedial actions when deficiencies are discovered?
6. Does the bank ensure that the third party selects an appraiser or a person to perform an evaluation who is competent, qualified, independent, and appropriately licensed or certified for a given assignment?
7. Does the bank ensure that the third party conveys to the appraiser or the person who performs the evaluation that the bank is the client?

ANALYTICAL METHODS AND TECHNOLOGICAL TOOLS

1. Does the bank have staff, or if necessary engage a third party, with the requisite expertise and training to manage the selection, use, and validation of an analytical method or technological tool?
2. Does the bank have adequate policies, procedures, and internal controls governing the selection, use, and validation of the valuation method or tool for the development of an evaluation?
3. Does the bank have appropriate policies and procedures governing the selection of automated valuation model (AVM)? For instance, did the bank:
   - Perform the necessary level of due diligence in selecting an AVM vendor and its models, considering how model developers conducted performance testing as well as the sample size used and the geographic level tested (such as county level or zip code).
   - Establish acceptable minimum performance criteria for a model prior to, and independent of, the validation process.
   - Perform validation of the model(s) during the selection process and document the validation process.
   - Evaluate underlying data used in the model(s), including the data sources and types, frequency of updates, quality control performed on the data, and the sources of the data in states where public real estate sales data are not disclosed.
   - Assess modeling techniques and the inherent strengths and weaknesses of different model types as well as how a model(s) performs for different property types.
   - Evaluate the AVM vendor's scoring system and methodology for the model(s).
   - Determine whether the scoring system provides an appropriate indicator of model reliability by property types and geographic locations.
4. Does the bank have procedures for monitoring the use of an AVM(s), including an ongoing validation process?
5. Does the bank maintain AVM performance criteria for accuracy and reliability in a given transaction, lending activity, and geographic location?

6. Has the bank established a criteria for determining whether a particular valuation method or tool is appropriate for a given transaction or lending activity, considering associated risks, including transaction size and purpose, credit quality, and leverage tolerance (loan-to-value)?
7. Does the criteria consider when market events or risk factors would preclude the use of a particular method or tool?
8. Does the bank have internal controls to preclude "value shopping" when more than one AVM is used for the same property?
9. Do the bank's policies include standards governing the use of multiple methods or tools, if applicable, for valuing the same property or to support a particular lending activity?
10. Does the bank have appropriate controls to ensure that the selected method or tool produces a reliable estimate of market value that supports the bank's decision to engage in a transaction?
11. Do the bank's policies and procedures adequately address the extent to which
    - An inspection or research should be performed to ascertain the property's actual physical condition, and
    - Supplemental information should be obtained to assess the effect of market conditions or other factors on the estimate of market value.

The Federal Reserve System relies on the timely and accurate filing of regulatory reports by domestic and foreign financial institutions. Data collected from regulatory reports facilitate early identification of problems that can threaten the safety and soundness of reporting institutions; ensure timely implementation of the prompt-corrective-action provisions required by law; and serve other legitimate supervisory purposes. Certain regulatory report information is used for public disclosure so investors, depositors, and creditors can better assess the financial condition of the reporting banks. Information that comes primarily from the Consolidated Reports of Condition and Income (Call Reports) is used to prepare the Uniform Bank Performance Report (UBPR), which employs ratio analyses to detect unusual or significant changes in a bank's financial condition as of the reporting dates. The UBPR is also used to detect changing patterns of behavior in the entire banking system; consequently, any inaccurate data in the regulatory reports may result in ratios that conceal deteriorating trends in the bank or the industry.

Generally, all regulatory reports of financial condition and income that domestic and foreign banking organizations file with the Federal Reserve are required by statute or regulation. The Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) and the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) amended various banking statutes to enhance the Federal Reserve's authority to assess civil money penalties against state member banks, bank holding companies, and foreign institutions that file "late," "false," or "misleading" regulatory reports. The civil money penalties also can be assessed against individuals who cause or participate in such filings.

The Federal Reserve has identified a late regulatory report as an official copy of a report that is not received by the Reserve Bank or its designated electronic collection agent in a timely manner. Each bank must file its Call Report in one of the following two ways:

- A bank may use computer software to prepare its report and then submit the report directly to the Federal Financial Institutions Examination Council's (FFIEC) Central Data Repository (CDR), an Internet-based system for data collection or
- The institution may complete its reports in paper form and arrange with a software vendor or another party to convert its paper reports into the electronic format that can be processed by the CDR. The software vendor or other party then must electronically submit the data file containing the bank's Call Report to the CDR.

The filing of a Call Report in paper form directly with the FDIC or with the appropriate Federal Reserve Bank is not an acceptable method of submission.

Reserve Banks will monitor the filing of all regulatory reports to ensure that they are filed, as required, on a timely basis and that they are accurate and not misleading. The Federal Reserve System's Committee on Current Series Reporting, which consists of staff from the statistics functions at each of the Reserve Banks and at the Board, will play an active role in this process. (See SR-04-15.) Many reporting errors can be screened through validity edit checks. Also, Reserve Banks have additional monitoring procedures that they use to confirm the timely submission of reports and to confirm that the reports are accurate and not misleading. On a case-by-case basis, the Reserve Banks will continue to determine if and when a financial institution or other banking organization is a chronic late, inaccurate, or false reporter; in these cases, the Banks will determine what supervisory action, if any, to recommend for a noncompliant reporter.

The filing of a false report generally involves the submission of mathematically incorrect data, such as addition errors or transpositions, or the submission of a regulatory report without its appropriate schedules. Conversely, the filing of a misleading report involves some degree of negligent behavior on the part of the filer that results in the submission of inaccurate information to the Federal Reserve.

REVIEW AND REFILING OF REGULATORY REPORTS

Review of regulatory reports involves determining whether the management of the member bank has submitted all required reports to the Federal Reserve in a timely and accurate man-

ner. The examiner assigned to a specific area of examination is responsible for reviewing the reports relating to that area and for verifying that they are accurate and meet statutory and regulatory requirements. If the examiner finds a material difference in the reports, management should be instructed to refile corrected copies, if appropriate.

Examiners should discuss on the "Examination Conclusions and Comments" and "Matters Requiring Board Attention" pages of the examination report material errors or the filing of chronically late reports. (See section 6000.1.) They should also discuss with Reserve Bank staff any regulatory report filing that is considered misleading, such a report could lead to the issuance of criminal referrals against the involved individuals. In addition, management should be reminded that civil money penalties or other enforcement proceedings could occur as a result of chronically late or false regulatory report filing.

Banks should maintain effective manual or automated internal systems and procedures to ensure that reporting meets the appropriate regulatory requirements. Banks should develop clear, concise, and orderly workpapers to support the compilation of data. Preparation of proper workpapers provides not only a logical tie between report data and the bank's financial records but also facilitates accurate reporting and verification. Ideally, as part of an effective internal control program, bank management should implement a procedure to verify the compilation of the data. At a minimum, an independent person or department should verify the data that have been compiled for inclusion in the report.

A bank's internal control and audit programs for regulatory reports should be sufficient to ensure that all required reports are submitted on time and are accurate. The specific internal controls a bank employs to meet those objectives depend largely on the volume of reports, the scope of a bank's operations, and the complexity of its accounting system.

COMMONLY REQUIRED REGULATORY REPORTS

This section describes the regulatory reports most commonly required either to be submitted by the member bank to the Federal Reserve Bank or the Board, or to be maintained by the member bank for review during an examination.

Consolidated Reports of Condition and Income

Under 12 USC 324 and the Board's Regulation H, all state member banks are required to file Consolidated Reports of Condition and Income (Call Reports) as of the last day of each calendar quarter. The specific reporting requirements, including the reporting form to be used (for example, FFIEC 031 or FFIEC 041), depend on the asset size of the bank and whether it has a foreign office. Details of the appropriate reporting guidelines, along with the specific reporting form to be filed, are found in the instructions for preparation of Reports of Condition and Income. The reporting forms and instructions can be found on the FFIEC's website: www.ffiec.gov.

The bank should submit completed Call Reports to the CDR no later than 30 calendar days after the report date. Any bank with more than one foreign office, other than a shell branch or international banking facility, must submit data to the CDR no later than 35 days after the report date. State member banks are *not* required to publish their Reports of Condition or Income, according to federal statute. However, a state member bank may be required to publish its Report of Condition under state law.

The Report of Condition provides consolidated, detailed financial information on assets, liabilities, capital, and off-balance-sheet activity, which permits a uniform analysis and comparison of the reporting bank's data to that of other insured banks. The report also aggregates certain figures on loans to executive officers, directors, principal shareholders, and their related interests. The Report of Income provides information such as consolidated earnings, changes in capital accounts and the allowance for loan and lease losses, and charge-offs and recoveries.

The examiner should carefully review both reports to ensure that all pertinent data have been reported and are properly categorized in accordance with the instructions. To understand a particular bank's Call Report, the examiner must understand the bank's accounting methods as well as the information located in, and the relationships between, the bank's general books and subsidiary ledgers. This understanding can be obtained only by a careful review of the

workpapers used in the preparation of these reports and their supplementary schedules.

REPORTS REQUIRED BY THE MONETARY CONTROL ACT OF 1980 AND THE INTERNATIONAL BANKING ACT OF 1978

The Federal Reserve has established a basic deposits-reporting framework for administering Regulation D, Reserve Requirements of Depository Institutions, and for constructing, analyzing, and controlling the monetary and reserves aggregates. The framework consists of four categories of deposit reporting. Every institution is placed into one of these four categories for deposit reporting purposes.[1] In general, the larger the institution, the more detailed or more frequent the institution will have to report.

The first two reporting categories, characterized as "detailed reporting," apply to those institutions that are not exempt from reserve requirements ("non-exempt" institutions). The last two reporting categories, characterized as "reduced reporting," apply to institutions that are exempt from reserve requirements ("exempt" institutions). The reserve-requirement "exemption amount" is the amount of total reservable liabilities at each depository institution that is subject to a zero-percent reserve requirement. The exemption amount is used to make the distinction between detailed deposit reporting and reduced reporting.

- Institutions with net transaction accounts equal to or less than the exemption amount over prescribed periods are exempt from reserve requirements and are subject to reduced reporting (categories 3 and 4).
- Institutions with net transaction accounts greater than the exemption amount over prescribed periods are *not* exempt from reserve requirements and are subject to detailed reporting (categories 1 and 2).

Both measures are indexed annually; see Regulation D for the appropriate exemption and cutoff amounts.

The exemption amount and the deposit cutoff for any one calendar year are used by the Federal Reserve to determine deposit-reporting panels in July, effective for September of that year, which continues to September of the following year. All deposit reports are mandatory.

Reporting Categories

"Non-exempt" institutions subject to detailed reporting file the Report of Transaction Accounts, Other Deposits and Vault Cash (FR 2900). Institutions file the report either weekly or quarterly, generally depending on the level of an institution's deposits. The report is used in the calculation of reserve requirements.

"Exempt" institutions subject to "reduced reporting" file either the Annual Report of Deposits and Reservable Liabilities (FR 2910a) or no report at all, depending on their deposit levels.

Report forms and instructions can be found on the Federal Reserve Board's website.

Category One

Depository institutions (other than banking Edge and agreement corporations and U.S. branches and agencies of foreign banks) with net transaction accounts greater than the exemption amount and with a sum of total transaction accounts, savings deposits, and small time deposits greater than or equal to the nonexempt deposit cutoff, or with a sum of total transaction accounts, savings deposits, and small time deposits greater than or equal to the reduced reporting limit, regardless of the amount of net transaction accounts, will be required to submit the FR 2900 weekly.

Banking Edge and agreement corporations and U.S. branches and agencies of foreign banks, regardless of size, must also submit the FR 2900 weekly. They are not eligible for reporting categories 2 through 4 below.

The weekly reporting period for the FR 2900 covers the seven-day period beginning on Tuesday and ending the following Monday.

Category Two

Depository institutions with net transaction accounts greater than the exemption amount and with a sum of total transaction accounts, savings deposits, and small time deposits less than the

1. Depository institutions that are required to maintain reserves are defined in section 204.1(c) of Regulation D (12 CFR 204.1(c)).

nonexempt deposit cutoff are required to submit the FR 2900 once each quarter, in March, June, September, and December.

The quarterly reporting period for the FR 2900 covers the seven-day period beginning on the third Tuesday of the report month and ending the following Monday.

Category Three

Depository institutions with net transaction accounts less than or equal to the exemption amount and with total deposits greater than the exemption amount but with total transaction accounts, savings deposits, and small time deposits below the reduced reporting limit are required to submit the FR 2910a. This report is filed as of June 30 each year.

Category Four

Depository institutions whose net transaction accounts and total deposits are less than or equal to the exemption amount are not required to submit any Federal Reserve deposit report as long as data on the level of an institution's deposits are readily available on a condition report.

Institutions for which deposit data are not readily available on a condition report will be required to submit the FR 2910a report to determine the appropriate reporting category.

See page IV-4 and IV-5 of the Federal Reserve's *Reserve Maintenance Manual* at http://www.frbservices.org/files/regulations/pdf/rmm.pdf.

Annual Panel Determinations

Each year the Federal Reserve reviews the institutions in the four reporting categories, and reassignments of institutions ("panel shifts") are determined each July and become effective in September. The panel shifts reflect movements in each individual depository institution's total deposits or total reservable liabilities across the prevailing boundaries (the exemption amount and the deposit cutoff) that separate the reporting categories. Documentation is available on the Federal Reserve's procedures (including the reports, data items, and reporting periods) for measuring an institution's total reservable liabilities and total deposits against the prevailing cutoffs for the annual panel determinations. Two special types of panel shifts are described below.

- *Voluntary shifts.* In July, the Federal Reserve informs each institution of its particular reporting requirement effective for September of that year to September of the following year. Any depository institution assigned to one particular category may elect instead to report deposits (and, if appropriate, to maintain reserves) in accordance with a higher-level category. (For example, an institution assigned to the FR 2900 quarterly reporting category may elect instead to report the FR 2900 weekly.) However, any such voluntary shifts may take place only once a year during the normal September panel shifts. Voluntary shifts to a lower-level category are not permitted.

- *Fast-growing institutions.* The Federal Reserve may require a depository institution that is experiencing above-normal growth to report on a more detailed or frequent basis before the September panel shifts.

For more detailed information, see the Federal Reserve's "Reserve Maintenance Manual."

REPORTS REQUIRED UNDER REGULATION H AND THE SECURITIES EXCHANGE ACT OF 1934

Section 12(i) of the Securities Exchange Act of 1934 (the 1934 act), as amended by the Sarbanes-Oxley Act of 2002, vests the Board with the authority to administer and enforce certain provisions of the 1934 act and the Sarbanes-Oxley Act with respect to state member banks that have a class of securities registered under section 12(b) or 12(g) of the 1934 act (registered state member banks). In particular, the Board is charged with enforcing sections 12, 13, 14(a), 14(c), 14(d), 14(f), and 16 of the 1934 act and sections 301, 302, 303, 304, 306(a), 401(b), 404, 406, and 407 of the Sarbanes-Oxley Act[2] with respect to registered state member banks. Sec-

2. See 15 USC 78j-1, 78*l*–78n, 78p, 7241–7244(a), 7261(b), 7262, 7264, and 7265.

tion 208.36(a) of Regulation H, which implements these provisions, generally requires registered state member banks to comply with any rules, regulations, and reporting forms adopted by the Securities and Exchange Commission (SEC) under the above-listed sections of the 1934 act and the Sarbanes-Oxley Act. (See 12 CFR 208.36(a), as amended by 68 *Fed. Reg.* 4096 (January 28, 2003).) Registered state member banks, however, generally must file any forms or reports required by these rules with the Board, rather than the SEC.

If a state member bank has a class of securities registered under section 12 of the 1934 act and, thus, is a registered state member bank, the examiner should consult with the bank's management to ensure that the reports required by Regulation H are properly filed with the Board. Listed below are a few of the most common forms and reports that must be filed with the Board by a registered state member bank pursuant to Regulation H. This list, however, is not exclusive and examiners should consult Board staff or Regulation H, the 1934 act, the Sarbanes-Oxley Act, and the SEC's implementing rules if questions arise concerning the filing of reports by a registered state member bank. See the list of reporting forms and the individual reporting forms and instructions on the SEC's website: www.sec.gov.

Section 12 of the 1934 Act

Form 8-A is for the registration of certain classes of securities pursuant to sections 12(b) or 12(g) of the 1934 act for, among other things, listing on national securities exchanges. Form F-10 is the general reporting form for registration of securities pursuant to the 1933 act and sections 12(b) or 12(g) of the 1934 act for classes of securities of issuers for which no other reporting form is prescribed.

Section 13 of the 1934 Act

Form 8-K must be filed within 4 business days after the occurrence of the earliest of one or more specified events that are required to be reported and that affect the bank or its operations, such as changes in control of registrant or an acquisition or disposition of a significant amount of assets. See the "Information to be Included in the Report" within the report instructions. Form 10-Q is for quarterly and transition reports and must be filed within 40 days for large accelerated filers; accelerated filers; or for others, 45 days after the end of each of the first three fiscal quarters. Form 10-K is for annual and transition reports that must be filed within 60 to 90 calendar days after the end of the registrant's fiscal year.

Section 16 of the 1934 Act

Section 16 requires the directors, officers, and principal shareholders of public companies to file reports concerning the purchase and sale of the company's equity securities. Form 3 collects the insider's initial beneficial ownership of registered companies, including banks. Form 4 collects changes in the insider's beneficial ownership. Form 5 is an annual statement of changes in beneficial ownership of securities.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act[3] (the act) and the SEC's implementing rules require the principal executive officer and principal financial officer of public companies to file certain certifications with the company's annual 10-K report and quarterly 10-Q reports. The certifications must, among other things, state that the officer has reviewed the report, indicate that the report (to the officer's knowledge) does not contain any material misstatements or omissions, and contain certain representations concerning the company's internal controls.

The act requires the annual 10-K report of public companies to include a statement of management's responsibility for maintaining adequate internal-control structures and procedures for financial reporting and to contain an assessment of the effectiveness of these controls and procedures.[4] The company's external auditor must attest to, and report on, management's assessment. These reports and attestations are similar to the internal-control reports and attestations required by section 36 of the Federal Deposit Insurance Act (12 USC 1831m) for insured depository institutions with total assets of $500 million or more.

3. See 15 USC 7241 (section 302 of the act).
4. See 15 USC 7262 (section 404 of the act).

The act[5] and the SEC's rules also require public companies to disclose in their periodic reports whether the company has adopted a code of ethics for its senior financial officers and whether the company's audit committee includes a "financial expert." If the company has not adopted a code of ethics or does not have a financial expert on its audit committee, the company must explain the reasons why not.

REPORTING AND INQUIRY REQUIREMENTS FOR LOST AND STOLEN SECURITIES

Every national securities exchange member, registered securities association member, broker, dealer, municipal securities dealer, government securities broker or dealer, registered transfer agent, and registered clearing agency and its participants, as well as every member bank of the Federal Reserve System and every bank whose deposits are insured by the Federal Deposit Insurance Corporation (reporting institutions), must register with the SEC's designee, the Securities Information Center, Inc. (SIC). All lost, missing, stolen, or counterfeit securities must be reported to the SIC. Except in certain limited circumstances, each insured bank is responsible for contacting the SIC to determine if the securities coming into its possession, whether by pledge, transfer, or some other manner, have been previously reported as missing, lost, stolen, or counterfeit.

All functions within a bank that handle or process securities are subject to the *reporting* requirements. Only the transfer-agent function is exempt from the *inquiry* requirements. Accordingly, all bank departments likely to be affected, including the trust, investment, transfer-agent, custody, or dealer departments, and the lending operations as relating to collateral loans, should be familiar with the requirements set out in 17 CFR 240.17f-1. Securities exempt from the reporting requirements are—

- registered U.S. Treasury securities of the U.S. government and federal agencies thereof,
- securities that have not been assigned CUSIP numbers, and
- bond coupons
- global securities
- uncertified securities, and
- any securities issue for which there is neither a record nor beneficial owners that can obtain negotiable securities certificates.

Securities exempt from the inquiry requirements are—

- securities received directly from the issuer or its agent at issuance,
- securities received from another reporting institution or from a Federal Reserve Bank or Branch,
- securities received from a customer of the reporting institution in the name of the customer or nominee, and
- securities that are a part of a transaction of $10,000 or less (aggregate face value for bonds or market value for stocks).

Lost, Missing, Stolen, or Counterfeit Securities

Form X-17F-1A must be filed with the SIC within one business day after the discovery of—

- a theft or loss of any security when there is a substantial indication of criminal activity,
- a security that has been lost or missing for two business days when criminal actions are not suspected, and
- a security that is counterfeit.

The reporting form must be filed within two business days of notification of nonreceipt when delivery of securities sent by the bank—

- is made by mail or draft and payment is not received within 10 business days, and confirmation of nondelivery has been made by the receiving institution; and
- is in person and no receipt is maintained by the bank.

If securities sent by the bank, either in person or through a clearing agency, are lost in transit and the certificate numbers of the securities can be determined, the bank (delivering institution) must report the certificate numbers of the securities within two business days after notice of non-receipt or as soon as the certificate numbers of the securities can be ascertained.

5. See 15 USC 7264–7265 (sections 406 and 407 of the act).

When a shipment of retired securities certificates is in transit between any unaffiliated transfer agents, banks, brokers, dealers, or other reporting institutions, and the delivering institution fails to receive notice of receipt or nonreceipt of the certificates, the delivering institution is required to act to determine the facts. When the certificates are not recovered by the delivering institution, the delivering institution must report the certificates as lost, stolen, or missing within a reasonable time period, but in any event within twenty business days from the date of shipment. The delivery of lost or missing securities to the bank must be reported within one business day after discovery and notification of certificate numbers. Securities that are considered lost or missing as a result of count or verifications must be reported no later than 10 business days after discovery or as soon as certificate numbers can be ascertained.

Copies of all reports required to be filed under 17 CFR 240.17f-1 must also be submitted to the registered transfer agent for the issue being reported and, if criminal activities are suspected, to the Federal Bureau of Investigation. Copies of filed or received Forms X-17F-1A must be maintained in an easily accessible place for three years.

TRANSFER-AGENT ACTIVITIES

If a bank acts as a transfer agent for its own stock, the stock of its holding company, or any other equity security, it may have to register with the Board as a transfer agent pursuant to the requirements of Regulation H (section 208.31). State member bank transfer agents must comply with the SEC's rules prescribing operational and reporting requirements, which the SEC adopted pursuant to section 17A(2) of the 1934 act (15 USC 78q-1). For member banks, see 17 CFR 240.17Ac2 (1-2) and 240.17Ad-1-240.17Ad-16). (See section 208.31(b) of Regulation H.) Any entity performing transfer agent functions for a security is required to register if the security is registered on a national securities exchange and if the issuer has total assets of $10 million and a class of equity security held on record by 500 or more persons. The registrations are public filings and are *not* confidential.

The interagency Transfer Agent Registration and Amendment Form, Form TA-1, is used by member banks and other entities to register before becoming, and then to act as, a transfer agent. They also use the reporting form to amend registration information as necessary. The information collected includes the company name, all business addresses, and information about the registrant's proposed activities as a transfer agent.

The Federal Reserve uses the information to act upon registration applications and to aid in performing supervisory duties. The Federal Reserve forwards copies of the completed registration forms to the Securities and Exchange Commission, which maintains registration data to aid in its statutory mandate to develop rules and standards applicable to all registered transfer agents.

Municipal Securities Dealer Activities

A state member bank, subsidiary, department, or division thereof that is a municipal securities dealer must register and file amendments with both the SEC and the Federal Reserve Board Board as a municipal securities dealer by filing the SEC's Form MSD, pursuant to Section 15 B(a) of the Securities Exchange Act of 1934 and the SEC's rule 15Ba2-1. A discussion of the bank's responsibilities as a municipal securities dealer, filing requirements, and other information, including examination procedures, are discussed in section 2030.1. A notice of withdrawal from registration as a municipal securities dealer pursuant to section 15B(c) must be filed with the SEC and the Board on the SEC's Form MSDW when the municipal securities dealer is a bank, or a separately identifiable department or division of a bank.

Government Securities Broker and Dealer Activities

If a state member bank, a foreign bank, a state branch or an agency of a foreign bank, or a commercial lending company owned or controlled by a foreign bank acts as a government securities broker or dealer, it may have to file notice with the Board as a government securities broker or dealer by filing FR G-FIN, pursuant to section 15C(a)(1)(B) of the Securities and Exchange Act of 1934. This notice collects the institution's identifying information and the names and titles of its managers of government

securities activities; the notice requires the institution to state whether any person associated with the respondent's government securities activities has been involved in disciplinary proceedings related to securities sales. When such a financial institution intends to cease engaging in broker or dealer activities, it must notify its regulator by using the Notice by Financial Institutions of Termination of Activities as a Government Securities Broker or Government Securities Dealer (FR G-FINW). A discussion of the bank's responsibilities as a government securities broker or dealer, filing requirements, and other information, including examination procedures, are discussed in SR-87-37, as amended. See also SR-94-5, 93-40, 90-1, and 88-26. The Board has also developed a Summary Report of Government Securities Broker/Dealer Activities (GSB-D report).

INTERNATIONAL ACTIVITIES

A bank must file certain reports if it is conducting or intends to conduct international activities through either foreign branches or Edge Act or agreement corporations. Listed below is a brief description of each of these reports.

FFIEC 009—Country Exposure Report

FFIEC 009 is filed quarterly by all U.S. banks and bank holding companies that meet certain ownership criteria and that, on a fully consolidated basis, have total outstanding claims of $30 million or more (or equivalent) on foreign residents of the U.S. Information is collected on the distribution by country of these foreign claims on foreigners held by U.S. banks and bank holding companies.

FFIEC 009a—Country Exposure Information Report

FFIEC 009a is a quarterly supplement to the Country Exposure Report (FFIEC 009) that provides specific information about the reporting institution's exposures in particular countries of U.S. banking institutions. Part A must be filed when exposure to a single country exceeds 1 percent of the banking institution's total assets or 20 percent of that institution's capital, whichever is less. Part B provides a list of countries where exposures were between 0.75 percent and 1 percent of the respondent's assets or between 15 percent and 20 percent of capital.

FFIEC 030/FFIEC 030S—Foreign Branch Report of Condition/Abbreviated Foreign Branch Report of Condition

These reports collect information on the structure and geographic distribution of foreign branch assets, liabilities, derivatives, and off-balance-sheet data of foreign branches of insured U.S.-chartered commercial banks. For purposes of this report, branches in Puerto Rico and other U.S. territories and possessions are considered foreign branches. Participation in the completion and submittal of the reports is mandatory.

The FFIEC 030 is filed quarterly for significant branches, with either $2 billion or commitments to purchase foreign currencies and U.S. dollar exchange of at least $5 billion. It is filed annually for other branches with total assets in excess of $250 million. The Federal Reserve uses the data to plan examinations and to analyze the foreign operations of domestic banks. Growth trends can be measured by bank, by country, and by bank within country. Aggregate data are a useful source of information on bank activities.

The FFIEC 030S collects financial data items for smaller, less-complex branches. It is filed annually, as of December 31, for foreign branches that do not meet the criteria to file the FFIEC 030 but have total assets of $50 million or more (but less than or equal to $250 million).

FR 2064—Recordkeeping Requirements

Effective September 1, 2001, the FR 2064 reporting form was replaced with a recordkeeping requirement and certain structure information was moved to the FR Y-10, Report of Changes in Organizational Structure. Internationally active U.S. banking organizations are still expected to maintain adequate internal records to allow examiners to review compliance with the investment provisions of Regulation K, under

the recordkeeping requirements of FR 2064 (no form is associated with this recordkeeping requirement). For each investment made under subpart A of Regulation K, records should be maintained on the type of investment (for example, equity (voting shares, nonvoting shares, partnerships, interests conferring ownership rights, participating loans)), binding commitments, capital contributions, and subordinated debt), the amount of the investment, the percentage ownership, activities conducted by the company and the legal authority for such activities, and whether the investment was made under general-consent, prior-notice, or specific-consent authority. For those investments made under general-consent authority, information also must be maintained that demonstrates compliance with the various limits set out in sections 211.8 and 211.10 of Regulation K.

Information maintained by the banking organization should be made available to examination staff during the course of on-site examinations and pursuant to other supervisory requests. The recordkeeping must be adequate to permit examiners to determine compliance. Examiners are expected to review a sample of these investments to determine the accuracy of the organization's records and to determine compliance with the regulation. (See SR-02-2.)

FR 2314/FR 2314S—Financial Statements of Foreign Subsidiaries of U.S. Banking Organizations

The FR 2314 is reported quarterly or annually, as of the last calendar day of the quarter, based on certain threshold criteria. The FR 2314 collects selected financial information for direct or indirect foreign subsidiaries of U.S. state member banks, Edge and agreement corporations, and bank holding companies. The FR 2314 consists of a balance sheet and income statement; information on changes in equity capital, changes in the allowance for loan and lease losses, off-balance-sheet items, and loans; and a memoranda section. The FR 2314S should be filed annually as of December 31 and collects four financial data items for smaller, less complex subsidiaries.

FR 2502q—Quarterly Report of Assets and Liabilities of Large Foreign Offices of U.S. Banks

The FR 2502q report is to be submitted by U.S. head offices of bank holding companies, commercial banks, and Edge and agreement corporations that file for their major foreign branches and large banking subsidiaries. It provides a geographic breakdown of each office's assets and liabilities. Branches of a U.S. bank with $500 million or more in total assets and foreign banking subsidiaries with $2 billion or more in total assets, or $10 million in deposit liabilities, are required to file this report quarterly.

FR 2886b—Consolidated Report of Condition and Income for Edge Act and Agreement Corporations

FR 2886b covers the operations of the reporting corporation, including any international banking facilities of the reporter. Corporations engaged in banking must submit the data at least quarterly.

FR 2915—Report of Foreign Currency Deposits

FR 2915 collects seven-day averages of the amounts outstanding of foreign currency–denominated deposits held at U.S. offices of the depository institution, converted to U.S. dollars and included in the Report of Transaction Accounts, Other Deposits and Vault Cash (FR 2900). The report is collected with the reporting week that begins the third Tuesday of March, June, September, and December.

FR Y-10—Report of Changes in Organizational Structure

The Y-10 is used to report, among other things, information on worldwide organizational structure of bank holding companies (BHCs), member banks, Edge and agreement corporations, and the U.S. operations of foreign banking organizations (FBOs)[6]. The reporting form

6. An FBO with U.S. operations that is not or ceases to be a "qualifying foreign banking organization" (QFBO) within the meaning of Regulation K, and is not otherwise treated as

includes detailed information on the structure of top-tier BHCs organized under U.S. or foreign law that are not FBOs, regardless of financial holding company (FHC) status; FBOs (both qualifying and nonqualifying) whether or not a BHC; state member banks not controlled by a BHC or FBO; Edge and agreement corporations not controlled by a BHC, FBO, or member bank; and nationally chartered banks not controlled by a BHC or FBO, but only with respect to their foreign investments. Within 30 calendar days of the event, banking organizations are required to report changes in investments as well as new activities (both foreign and domestic) on the FR Y-10 report. The reporting form includes the structure information on changes in FBOs (formerly the FR Y-10F) and the change in status of foreign branch of U.S. banking organizations (formerly the FR 2058).

The Board has placed greater importance on monitoring the level of international investments to ensure compliance with relevant banking laws and regulations, and to ensure that banking organizations do not expose themselves to undue risk. Examiners and other Federal Reserve System staff have a continuing need to monitor compliance with the Federal Reserve Act and sections 211.8–211.10 of the revised Regulation K.

Investments of less than 25 percent of the voting shares of a foreign nonbanking company are reported on the FR Y-10.[7] However, using the FR Y-6 (Annual Report of Bank Holding Companies) and the FR Y-7 report (Annual Report of Foreign Banking Organizations), banking organizations are required to report annually all investments, including those between 5 percent and 25 percent of voting shares.[8] The FR Y-6, FR Y-7, and the FR Y-10 collect information on structure and geographical information relating to foreign investments for ongoing monitoring.

Examiners are expected to review investment amounts and activities during the examination process. The portion of an examination dealing with Regulation K compliance should focus on confirming investments made pursuant to the general-consent provisions to meet the restrictions on investment amount and activities in sections 211.8–211.10 of Regulation K. Investments made under the general-consent provisions of Regulation K can be sizable, and thus can pose significant risk to the banking organization. Examiners should keep in mind that the Board has the authority to rescind an organization's general-consent investment privileges for various reasons, including safety-and-soundness concerns and noncompliance with the existing requirements of Regulation K. (See SR-02-2.)

Treasury International Capital Forms

The following reports are collected to gather information on international capital movements by U.S. banks and their Edge Act and agreement corporations, other depository institutions, international banking facilities, and bank holding companies.

BC: Report of U.S. Dollar Claims of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers, and Dealers on Foreigners

BL-1: Report of U.S. Dollar Liabilities of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers, and Dealers to Foreign-Residents

BL-2: Report of Customers' U.S. Dollar Liabilities to Foreigners

BQ-1: Report of Customers' U.S. Dollar Claims on Foreigners

BQ-2: Part 1. Report of Foreign Currency Liabilities and Claims of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers and Dealers, and of Their Domestic Customers vis-à-vis Foreigners

BQ-2: Part 2. Report of Customers' Foreign Currency Liabilities to Foreigners

BQ-3: Report of Maturities of Selected Liabilities of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers, and Dealers to Foreigners

a QFBO under Regulation K, should consult with Federal Reserve staff regarding the scope of its reporting obligations. In general, an FBO that is not or is not treated as a QFBO is subject to the nonbanking restrictions of the BHC Act with respect to its worldwide operations and, thus, would have to report on the FR Y-10 changes to its worldwide organizational structure.

7. Regulation K authorizes portfolio investments in less than 20 percent of the shares of a foreign company regardless of the activities engaged in by that company. Portfolio investments within the general-consent limits are required to be reported annually on the FR Y-6.

8. Investments representing less than 5 percent ownership are not required to be reported.

D: Report of Holdings of, and Transactions in, Financial Derivatives Contracts
S: Purchases and Sales of Long-Term Securities by Foreign-Residents
SHC/SHCA: Report of U.S. Ownership of Foreign Securities, Including Selected Money Market Instruments
SHL/SHLA: Foreign-Residents' Holdings of U.S. Securities, Including Selected Money Market Instruments

Consolidated Foreign Currency Reports of Major Market Participants

The Treasury Foreign Currency (TFC) Report of major market participants collects data on the foreign exchange contracts and actively manages positions of major nonbank market participants. This report is collected and processed by the Federal Reserve System, acting as fiscal agent for the Department of the Treasury. These data are designed to assess and monitor the foreign exchange developments in the spot, forward, futures, and options markets on an individual and aggregate basis. The TFC series is comprised of three reports: (1) the Weekly Consolidated Foreign Currency Report of Major Market Participants (TFC-1), (2) the Monthly Consolidated Foreign Currency Report of Major Market Participants (TFC-2), and (3) the Quarterly Consolidated Foreign Currency Report (TFC-3).

1. To determine that required reports are being filed on time.
2. To determine that the contents of reports are accurate.
3. To effect corrective action when official reporting, practices, policies, or procedures are deficient.

1. Complete or update the Internal Control Questionnaire, if selected for implementation.
2. Determine the bank's historical record of submitting timely and accurate reports by reviewing workpapers and the Regulatory Reports Monitoring Program.
3. Instruct those examiners assigned specific departments that generate regulatory reports to:
   a. Determine from department records what regulatory reports should have been filed because of the passage of time or the occurrence of an event.
   b. Obtain copies of all regulatory reports filed by the department since the previous examination.
   c. Check the reports obtained in the preceding step and the date of filing against statutory and regulatory requirements.
   d. Instruct the bank to prepare and submit any delinquent reports.
   e. For the most recent filing of those reports submitted on a periodic basis and all other reports submitted since the last examination, perform the following:
      - Reconcile the line items shown on the reports to the bank's general ledger, subsidiary ledgers, or daily statements.
      - Obtain the bank's workpapers applicable to each line item and reconcile individual items to the reports.
      - Determine whether other examining personnel uncovered any misstatement of assets, liabilities, income, or expense during their examination of the various departments.
      - Determine that the reports are prepared in accordance with Federal Reserve and/or other applicable instructions.
   f. On the basis of the work performed in the preceding step, perform either of the following, as appropriate:
      - If the reports are found to be substantially correct, limit the review of the remaining periodic reports filed since the last examination to the reconciliation of financial statement account categories to general ledger control accounts.
      - If the reports are found to be substantially incorrect, extend the procedures outlined in step 3.e to the remaining periodic reports filed since the last examination for those areas where items were found to be substantially incorrect.
   g. Scan all periodic reports for unusual fluctuations. Investigate fluctuations, if any.
4. Review compliance with the missing, lost, counterfeit, or stolen securities requirements of 17 CFR 240.17f-1 by:
   a. Discussing with appropriate officers and personnel the procedures in effect regarding the filing of Form X-17F-1A (Missing, Lost, Stolen, or Counterfeit Securities Report).
   b. Discussing with the appropriate persons the procedures in effect regarding compliance with the inquiry requirements.
   c. Substantiating Internal Control questions 6 through 15, as appropriate.
5. Prepare comments in appropriate report form and discuss with management:
   a. Violations of law or regulations.
   b. Inaccurate reports, and, if applicable, the need for amended reports. If amended reports are considered appropriate, consult with Reserve Bank supervisory personnel before requesting the bank to refile the report(s).
   c. Material differences in the annual report of the state member bank whose securities are subject to registration pursuant to the Securities Exchange Act of 1934. (State law governs the furnishing of annual reports to stockholders for banks with less than 500 shareholders.)
   d. Recommended corrective action when policies, practices, or procedures are deficient or when reports have been filed incorrectly, late, or not at all.

      The comments must include, if applicable, the name(s) and the "as of" date(s) of amended report(s); and the date of filing, amount of, and explanation of any material difference existing in either the numerical items or narrative statements in the annual report.
6. Update the workpapers with any information that will facilitate future examinations.

Review the bank's internal controls, policies, practices, and procedures for regulatory reports. The bank's system should be documented in a complete and concise manner and should include, where appropriate, narrative descriptions, flowcharts, copies of forms used, and other pertinent information.

1. Do requests for all regulatory reports come to one individual or department?
2. Does that individual or department have the authority to request that required information be prepared by the applicable banking department?
3. To ensure that all regulatory reports are submitted on a timely basis and are accurate, determine the following:
   a. If completion of the report requires information from several departments:
      - Is a written memorandum sent to the various departments requesting the information?
      - Is the memorandum addressed to a department head?
      - Does the memorandum have a due date?
      - Are procedures in effect to send second requests if the memorandum is not returned by its original due date?
      - Does completion of the memorandum require two signatures, that of the person gathering the information and that of the person's superior who is held responsible for its accuracy?
   b. If completion of the report requires information from one department, is there separation of duties to ensure that the raw data to complete the report is compiled by one person and verified by another person, prior to submission?
4. After the report is prepared, but prior to its submission, is it checked by:
   a. The supervisor of the department preparing the report, who takes personal responsibility for its accuracy and submission on a timely basis?
   b. Bank personnel who have no part in the report's preparation?
5. Do report workpapers leave a clear audit trail from the raw data to the finished report and are they readily available for inspection?

   Review the bank's system for compliance with the reporting and inquiry requirements of the lost and stolen securities provisions of 17 CFR 240.17f-1.
6. Has the bank registered as a direct or indirect inquirer with the Securities Information Center, Inc.?
7. Are reports submitted within one business day of discovery when:
   a. Theft or loss of a security is believed to have occurred through criminal activity?
   b. A security has been missing or lost for two business days, except in certain cases?
   c. A security is counterfeit?
8. Are reports submitted by the bank, as a delivering institution, within two business days of notification of nonreceipt when:
   a. Delivery is in person and no receipt is maintained by the bank?
   b. Delivery of securities is made by mail or via draft, and payment is not received within 10 business days and confirmation of nondelivery has been made by the receiving institution?
   c. Securities are lost in transit and the certificate number(s) can be determined?
9. Are reports submitted by the bank, as a receiving institution, within one business day of discovery and notification of the certificate number(s) when:
   a. Securities are delivered through a clearing agency and the delivering institution has supplied the certificate numbers within the required two business days after request?
   b. Securities are delivered over the window and the delivering institution has a receipt and supplies the certificate number(s) within the required two business days after request?
10. Are securities that are considered to be lost or missing as a result of counts or verifications reported no later than ten business days after discovery or as soon after as the certificate number(s) can be ascertained?
11. Are copies of those reports submitted to the registered transfer agent for the issue and, in

the case of suspected criminal activity, the Federal Bureau of Investigation?

12. Are all recoveries of securities reported within one business day of recovery or finding? (Note: Only the institution that initially reported the security as missing can make a recovery report.)
13. Are inquiries made when the bank takes in any security that is not:
    a. Received directly from the issuer or issuing agent at issuance?
    b. Received from another reporting institution or Federal Reserve bank in its capacity as fiscal agent?
    c. Received from a bank customer and is registered in the name of the customer or its nominee?
14. Are all reports made on Form X-17F-1A or facsimile?
15. Are copies of Form X-17F-1A and subsequent confirmations and other information received maintained for three years in an easily accessible location?

CONCLUSION

16. Does the foregoing information provide an adequate basis for evaluating internal controls in that deficiencies in areas not covered by this questionnaire do not significantly impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
17. Are internal controls adequate based on a composite evaluation, as evidenced by answers to the foregoing questions?

Sale of Uninsured Nondeposit Debt Obligations on Bank Premises

Effective date May 1996

Section 4160.1

INTRODUCTION

State member banks have, at times, engaged in issuing nondeposit debt securities on their own behalf or assisted in the sale of these instruments (for example, commercial paper or other short-term or long-term debt securities, such as thrift notes and subordinated debentures) on behalf of their parent bank holding companies or other affiliates. It is important to ensure that these securities are not issued, marketed, or sold in a manner that could give the purchaser the impression that the obligations are federally insured deposits. Consequently, state member banks and their subsidiaries that have issued or plan to issue nondeposit debt securities should not market or sell these instruments in any public area of the bank where retail deposits are accepted, including any lobby area of the bank.

PROCEDURES

This policy is not intended to prevent banks from selling their uninsured debt instruments in a manner that is consistent with sound and prudent banking practices. These instruments generally may be sold to investors in various ways away from the retail deposit-taking and general lobby areas of the bank. In this regard, personnel not regularly involved in deposit-taking activities or in opening new deposit accounts may make prospective investors in the community aware of uninsured debt obligations outside of the retail deposit-taking and general lobby areas. Also, these instruments may generally be sold by an employee or officer segregated from the retail deposit-taking and general lobby areas of the bank, even if the employee or officer occasionally accepts deposits or opens an account (but not as a part of his or her regular duties), so long as the arrangement is not structured in a way that misleads the purchaser or is otherwise contrary to supervisory guidelines.

Further, state member banks involved in this activity should establish procedures to ensure that potential purchasers understand that the debt security is not federally insured or guaranteed. Specifically, the debt security should boldly state on its face that it is not insured by the Federal Deposit Insurance Corporation. In addition, this information should be verbally stated to the purchaser, and, in cases where purchasers do not take physical possession of the obligation, the purchaser should be provided with printed advice that conveys this information.

SUPERVISORY GUIDANCE

As noted, a state member bank may also become involved in the sale of uninsured debt obligations of its parent bank holding company or a nonbank affiliate. It is a longstanding policy of the Federal Reserve that debt obligations of a bank holding company or a nonbank affiliate not be issued, marketed, or sold in a way that conveys the misimpression or misunderstanding that these instruments are either (1) federally insured deposits or (2) obligations of or guaranteed by the subsidiary bank. The purchase of these holding company obligations by retail depositors of the subsidiary bank can, in the event of default, result in losses to individuals who believed that they had acquired federally insured or guaranteed instruments. In addition to the problems created for these individuals, this situation could impair public confidence in the bank and lead to unexpected withdrawals or liquidity pressures.

If a state member bank intends to market or sell or to allow its parent holding company or a nonbank affiliate to market or sell uninsured nondeposit debt obligations on bank premises, the bank should establish internal controls to ensure that the promotion, sale, and subsequent customer relationship resulting from the sale of these debt obligations is separated from the retail deposit-taking functions of the bank. For further information on commercial paper, see section 2030, ‘‘Bank Dealer Activities.’’

Sale of Uninsured Nondeposit Debt Obligations on Bank Premises

Examination Objectives

Effective date May 1996

Section 4160.2

1. To determine if uninsured nondeposit debt obligations of the state member bank or an affiliate are sold on bank premises.
2. To determine if the policies, practices, procedures, and internal controls for the sale of uninsured nondeposit debt instruments are adequate.
3. To ensure that the marketing and sale of uninsured nondeposit debt instruments are not conducted in a manner that conveys the impression or suggestion that they are federally insured deposits. Additionally, holding company or affiliate instruments should not convey the impression or suggestion that they are obligations of or guaranteed by the state member bank.
4. To ensure that the marketing and sale of uninsured nondeposit debt obligations are sufficiently separated and distinguished from retail banking operations, particularly the deposit-taking function.
5. To initiate corrective action if policies, practices, or procedures related to the sale of uninsured nondeposit debt instruments are deficient.

Sale of Uninsured Nondeposit Debt Obligations on Bank Premises

Examination Procedures

Effective date September 1992

Section 4160.3

1. Verify that the bank does not sell uninsured nondeposit debt instruments at teller windows or other areas where retail deposits are routinely accepted, including general lobby areas surrounding teller windows and personal banking desks.
2. Assess the adequacy of disclosures and the separation of the marketing and sale of uninsured nondeposit debt obligations from the retail deposit-taking function by assuring that:
   a. the debt instrument, advertising, and all related documents disclose prominently in bold print that the debt instrument is not insured by the Federal Deposit Insurance Corporation (bank holding company debt instruments should also state that the instrument is not an obligation of, or guaranteed by, the bank);
   b. advertisements that promote uninsured debt obligations of the bank (or an affiliate) do not also promote insured deposits of the bank in a way that could lead to confusion;
   c. the obligor of the uninsured debt instrument is prominently disclosed and names or logos of the bank are not used on holding company or nonbank affiliate instruments in a way that might suggest the insured bank is the obligor;
   d. adequate verbal disclosures are made during telemarketing contacts and at the time of sale (a review of employee instructions or a telemarketing script, or appropriate questions directed to an employee handling this function, could assist an examiner in assessing the adequacy of verbal disclosure);
   e. retail deposit-taking employees of the insured depository institution are not engaged in the promotion or sale of uninsured nondeposit debt instruments;
   f. information on uninsured nondeposit debt instruments is not contained in the retail deposit statements of customers or in the immediate retail deposit-taking area; and
   g. account information on holdings of uninsured nondeposit debt instruments is not included on insured deposit statements.
3. Encourage the bank to obtain a signed statement from the customer indicating that the customer understands that the uninsured debt instrument is not a deposit and is not FDIC insured.

Depository institutions have become increasingly involved in selling uninsured nondeposit investment products, such as mutual funds or annuities, on their premises to retail customers. In response to this development, an interagency statement on retail sales of nondeposit investment products (interagency statement) was issued on February 15, 1994, to enhance customer protection and lessen possible customer confusion that these products are insured deposits.[1] The interagency statement applies to all insured banks and thrifts, including state member banks and the U.S. branches and agencies of foreign banks.

The guidelines contained in the interagency statement apply to retail recommendations or sales of nondeposit investment products made by—

- employees of a depository institution,
- employees of an affiliated or unaffiliated third party occurring on the premises of the banking organization (including telephone sales, investment recommendations by employees, and sales or recommendations initiated by mail from its premises), and
- sales resulting from a referral of retail customers by the institution to a third party when the depository institution receives a benefit for the referral.

Retail sales include (but are not limited to) sales to individuals by depository-institution personnel or third-party personnel conducted in or adjacent to a depository institution's lobby area. The sales of government and municipal securities made in a depository institution's dealer department located away from the lobby area are not subject to the interagency statement. In addition, the interagency statement generally does not apply to fiduciary accounts administered by a depository institution. However, for fiduciary accounts where the customer directs investments, such as self-directed individual retirement accounts, the disclosures prescribed by the interagency statement (see the "Disclosures and Advertising" subsection below) should be provided. Furthermore, the interagency statement applies to affiliated broker-dealers when the sales occur on the premises of the depository institution. The interagency statement also applies to sales activities of an affiliated broker-dealer resulting from a referral of retail customers by the depository institution.

The Rules of Fair Practice of the Financial Industry Regulatory Authority govern sales of securities by its member broker-dealers. In addition, the federal securities laws prohibit materially misleading or inaccurate representations in connection with the offer or sale of securities and require that sales of registered securities be accompanied by a prospectus that complies with SEC disclosure requirements.

Examiners should determine whether the institution has adequate policies and procedures to govern the conduct of the sales activities on bank premises and, in particular, whether sales of nondeposit investment products are distinguished from the deposit-taking activities of the bank through disclosure and physical means that are designed to prevent customer confusion.

Although the interagency statement does not apply to sales of nondeposit investment products to nonretail customers, such as fiduciary customers, examiners should also apply the examination procedures prescribed in SR-94-34 ("Examination Procedures for Retail Sales of Nondeposit Investment Products," May 26, 1994) when retail customers are directed to the institution's trust department, where they may purchase nondeposit investment products by simply completing a customer agreement.

PROGRAM MANAGEMENT

Banks must adopt policies and procedures governing nondeposit investment product retail sales programs. These policies and procedures should be in place before the commencement of the retail sale of nondeposit investment products on bank premises.

The bank's board of directors is responsible for ensuring that retail sales of nondeposit investment products comply with the interagency statement and with all applicable state and federal laws and regulations. Therefore, the

1. The interagency statement was issued to Federal Reserve Banks under cover of a supervisory letter, SR-94-11 ("Interagency Statement on Retail Sales of Nondeposit Investment Products," February 17, 1994). Additional guidance is provided in SR-95-46 ("Interpretation of Interagency Statement on Retail Sales of Nondeposit Investment Products," September 14, 1995).

board, or a designated committee of the board, should adopt written policies that address the risks and management of these sales programs. Policies and procedures should reflect the size, complexity, and volume of the institution's activities or, when applicable, the institution's arrangements with any third parties selling these products on bank premises. The bank's policies and procedures should be reviewed periodically by the board of directors, or its designated committee, to ensure that they are consistent with the institution's current practices, applicable laws, regulations, and guidelines.

A bank's policies and procedures for nondeposit investment products should, at a minimum, address (1) disclosure and advertising, (2) the physical separation of investment sales from deposit-taking activities, (3) compliance and audit requirements, (4) suitability concerns, and (5) other sales practices and related risks. In addition, policies and procedures should address the following areas.

Types of Products Sold

When evaluating nondeposit investment products, management should consider what products best meet the needs of the bank's customers. Policies should outline the criteria and procedures that will be used to select and periodically review nondeposit investment products that are recommended or sold on the bank's premises. Institutions should periodically review the products offered to ensure that they meet their customers' needs.

Use of Identical or Similar Names

Because of the possibility of customer confusion, a nondeposit investment product must not have a name that is identical to the name of the bank or its affiliates. However, a bank may sell a nondeposit investment product with a similar name as long as the sales program addresses the even greater risk that customers may regard the product as an insured deposit or other obligation of the bank. Moreover, the bank should review the issuer's disclosure documents for compliance with SEC requirements, which call for a thorough explanation of the relationship between the bank and the mutual fund.

The Federal Reserve applies a stricter rule to investment adviser activities under Regulation Y (12 CFR 225.125) when a bank holding company (as opposed to a bank) or nonbank subsidiary acts as an investment advisor to a mutual fund. In this case, the fund may not have a name that is identical to, similar to, or a variation of the name of the bank holding company.

Permissible Use of Customer Information

Banks should adopt policies and procedures on the use of confidential customer information for any purpose in connection with the sale of nondeposit investment products. The industry guidelines permit institutions to share with third parties only limited customer information, such as the name, address, telephone number, and types of products owned. The guidelines do not permit the sharing of more confidential information, such as specific or aggregate dollar amounts of investments or net worth, without the customer's prior acknowledgment and written consent.

Arrangements with Third Parties

A majority of all nondeposit investment products sold on bank premises are sold by representatives of third parties. Under these arrangements, the third party has access to the institution's customers, and the bank is able to make nondeposit investment products available to interested customers without having to commit the resources and personnel necessary to sell the products directly. Third parties include wholly owned subsidiaries of a bank, bank-affiliated broker-dealers (section 20 companies[2] or discount brokerage firms), unaffiliated broker-dealers, insurance companies, or other companies in the business of distributing nondeposit investment products on a retail basis.

Bank management should conduct a comprehensive review of an unaffiliated third party before entering into any arrangement. The review should include an assessment of the third party's

2. A nonbank subsidiary of a bank holding company that has been authorized to underwrite and deal in certain debt and equity securities that cannot be underwritten or dealt in by member banks directly.

financial status, management experience, reputation, and ability to fulfill its contractual obligations to the bank, including its compliance with the interagency statement.

Banks should enter into written agreements with any affiliated and unaffiliated third parties that sell nondeposit investment products on bank premises. These agreements should be approved by the bank's board of directors or its designated committee. Agreements should outline the duties and responsibilities of each party; describe third-party activities permitted on the institution's premises; address the sharing or use of confidential customer information for investment sales activities; and define the terms for use of the bank's office space, equipment, and personnel. If an arrangement includes dual employees (bank employees also utilized by a third party), the agreement must provide for written employment contracts that specify the duties of these employees and their compensation arrangements.

In addition, a third-party agreement should specify that the third party will comply with all applicable laws and regulations and will conduct its activities in a manner consistent with the interagency statement. The agreement should authorize the institution to monitor the third party's compliance with its agreement, as well as authorize the bank and Federal Reserve examination staff to have access to third-party records considered necessary to evaluate this compliance. These records should include examination results, sales practice reviews, and related correspondence provided to the third party by securities regulatory authorities. Finally, the agreement should provide for indemnification of the institution by an unaffiliated third party for the conduct of its employees in connection with its sales activities. Notwithstanding the provisions of a third-party agreement, bank management should monitor the conduct of nondeposit investment product sales programs to ensure that sales of the products are distinct from other bank activities and are not conducted in a manner that could confuse customers about the lack of insurance coverage for these investments.

Contingency Planning

Nondeposit investment products are subject to price fluctuations caused by changes in interest rates and stock market valuations. In the event of a sudden, sharp drop in the market value of nondeposit investment products, institutions may experience a heavy volume of customer inquiries, complaints, and redemptions. Therefore, management should develop contingency plans to address these situations. A major element of any contingency plan should be to provide customers with access to information about their investments. Other factors to consider in contingency planning include public relations and the ability of operations staff to handle increased volumes of transactions.

DISCLOSURES AND ADVERTISING

Content, Form, and Timing of Disclosures

Nondeposit investment product sales programs should ensure that customers are clearly and fully informed of the nature and risks associated with these products. In addition, nondeposit investment products must be clearly differentiated from insured deposits. The interagency statement identifies the following minimum disclosures that must be made to customers when providing investment advice, making investment recommendations, or effecting nondeposit investment product transactions:

- They are not insured by the FDIC.
- They are not deposits or other obligations of the institution and are not guaranteed by the institution.
- They are subject to investment risks, including the possible loss of the principal invested.

There are limited situations in which the disclosure guidelines need not apply or where a shorter logo format may be used in lieu of the longer written disclosures.

The interagency statement disclosures do not need to be provided in the following situations:

- radio broadcasts of 30 seconds or less;
- electronic signs,[3] and
- signs, such as banners and posters, when they are used only as location indicators.

3. "Electronic signs" may include billboard-type signs that are electronic, time-and-temperature signs, and ticker-tape signs. Electronic signs would not include such media as television, on-line services, or ATMs.

Additionally, third-party vendors not affiliated with the depository institution need not make the interagency statement disclosures on nondeposit investment product confirmations and in account statements that may incidentally, with a valid business purpose, contain the name of the depository institution.

Shorter, logo-format disclosures may be used in visual media, such as television broadcasts, ATM screens, billboards, signs, posters, and written advertisements and promotional materials, such as brochures. The text of an acceptable logo-format disclosure would include the following statements:

- Not FDIC-Insured.
- No Bank Guarantee.
- May Lose Value.

Disclosure is the most important way of ensuring that the differences between nondeposit investment products and insured deposits are understood by retail customers. Accordingly, it is critical that the minimum disclosures be presented clearly and concisely in both oral and written communications. In this regard, the minimum disclosures should be provided—

- orally during any sales presentations (including telemarketing contacts) or when investment advice is given,
- orally and in writing before or at the time an investment account to purchase these products is opened, and
- in all advertisements and other promotional materials (discussed further below).

The minimum disclosures may be made on a customer account agreement or on a separate disclosure form. The disclosures must be conspicuous (highlighted through bolding, boxes, and/or a larger typeface). Disclosures contained directly on a customer account agreement should be located on the front of the agreement or adjacent to the customer signature block.

Banks are to obtain a written acknowledgment—on the customer account agreement or on a separate form—from a customer confirming that he or she has received and understands the minimum disclosures. For nondeposit investment product accounts established before the issuance of the interagency statement, banks should obtain a disclosure acknowledgment from the customer at the time of the customer's next purchase transaction. If an institution solicits customers by telephone or mail, it should ensure that the customers receive the written disclosures and an acknowledgment to be signed and returned to the institution.

Customer account statements, including combined statements for linked accounts and trade confirmations that are provided by the bank or an affiliate, should contain the minimum disclosures if they display the name or logo of the bank or its affiliate. Statements that provide account information about insured deposits and nondeposit investment products should clearly segregate the information about nondeposit investment products from the information about deposits to avoid customer confusion.

Advertising

The interagency statement provides that advertisements in all media forms that identify specific investment products must conspicuously include the minimum disclosures and must not suggest or convey any inaccurate or misleading impressions about the nature of a nondeposit investment product. Promotional material that contains information about both FDIC-insured products and nondeposit investment products should clearly segregate the information about the two product types. When promotional sales materials related to nondeposit investment products are displayed in the bank's retail areas, they should be grouped separately from material related to insured bank products.

Telemarketing scripts should be reviewed to determine whether bank personnel are inquiring about customer investment objectives, offering investment advice, or identifying particular investment products or types of products. In these cases, the scripts must contain the minimum disclosures, and bank personnel relying on the scripts must be formally authorized to sell nondeposit investment products by their employers. Further, these personnel must have training that is the substantive equivalent of that required for personnel qualified to sell securities as registered representatives (see the "Training" subsection below).

Additional Disclosures

A bank should apprise customers of certain material relationships. For example, a customer

should be informed by sales personnel orally and in writing before the sale about any advisory relationship existing between the bank (or an affiliate) and a mutual fund whose shares are being sold by the institution. Similarly, fees, penalties, or surrender charges associated with a nondeposit investment product should be disclosed by sales personnel orally and in writing before or at the time the customer purchases the product. The SEC requires written disclosure of this information in the investment product's prospectus.

If sales activities include any written or oral representations concerning insurance coverage by any entity other than the FDIC (for example, SIPC insurance of broker-dealer accounts, a state insurance fund, or a private insurance company), then clear and accurate explanations of the coverage must also be provided to customers at that time to minimize possible confusion with FDIC insurance. These disclosures should not suggest that other forms of insurance are the substantive equivalent to FDIC deposit insurance.

SETTING AND CIRCUMSTANCES

Physical Separation from Deposit Activities

Selling or recommending nondeposit investment products on bank premises may give the impression that the products are FDIC-insured or are obligations of the bank. To minimize customer confusion with deposit products, nondeposit investment product sales activities should be conducted in a location that is physically distinct from the areas where retail deposits are taken. Bank employees located at teller windows may not provide investment advice, recommend investment products, or accept orders (even unsolicited orders) for nondeposit investment products.

To decide whether nondeposit investment product sales activities are sufficiently separate from deposit activities, the particular circumstances of each bank need to be evaluated. FDIC insurance signs and insured deposit-related promotional material should be removed from the investment product sales area and replaced with appropriate signs indicating that the area is used for the sale of investment products. Signs referring to specific investments should prominently contain the minimum disclosures. In the limited situation where physical constraints prevent nondeposit investment product sales activities from being conducted in a distinct and separate area, the institution has a heightened responsibility to ensure that appropriate measures are taken to minimize customer confusion.

In the case of banks that are affiliated with section 20 companies that sell retail investment products directly to bank customers, the requirement for separation of deposit-taking facilities from the securities operations of the section 20 company is absolute under the relevant firewall conditions imposed on these companies by the Board. Accordingly, retail sales activities conducted by a section 20 company must be in a separate office which, at a minimum, is set off from deposit-taking activities by partitions and identified by signs with the name of the section 20 company. Further, section 20 company employees may not be dual employees of the bank. Business cards for designated sales personnel should clearly indicate that they sell nondeposit investment products or, if applicable, are employed by a broker-dealer.

The interagency statement was intended generally to cover sales made to retail customers in the bank lobby. However, some institutions may have an arrangement whereby retail customers purchase nondeposit investment products at a location of the institution that is generally confined to institutional services (for example, corporate money desk). In these cases, the bank should still ensure that retail customers receive the minimum disclosures to minimize any possible customer confusion with nondeposit investment products and insured deposits.

Hybrid Instruments and Accounts

When an institution offers accounts that link traditional bank deposits with nondeposit investment products, such as a cash-management account,[4] the accounts should be opened in the investment sales area by trained personnel. In light of the hybrid characteristics of these products, the opportunity for customer confusion is amplified, and the institution should take special care during the account-opening process to ensure that a customer is accurately informed that

4. A hybrid account may incorporate deposit and brokerage services, credit/debit card features, and automated sweep arrangements.

- funds deposited into a sweep account will only be FDIC-insured until they are swept into a nondeposit investment product account and
- customer account statements may disclose balances for both insured and nondeposit product accounts.

DESIGNATION, TRAINING, AND SUPERVISION OF PERSONNEL

Hiring and Training of Sales Personnel

Banks hiring sales personnel for nondeposit investment product programs should investigate the backgrounds of prospective employees. When a candidate for employment has previous investment industry experience, the bank should check whether the individual has been the subject of any disciplinary actions by securities, state, or other regulators.

Unregistered bank sales personnel should receive training that is the substantive equivalent of that provided to personnel qualified to sell securities as registered representatives. Training should cover the areas of product knowledge, trading practices, regulatory requirements and restrictions, and customer-protection issues. In addition, training programs should cover the bank's policies and procedures for sales of nondeposit investment products and should be conducted continually to ensure that staff are familiar with new products and compliance issues.

For those bank employees whose sales activities are limited to mutual funds or variable annuities, the equivalent training is that ordinarily needed to pass NASD's series 6 limited representative examination, which typically involves approximately 30 to 60 hours of preparation, including about 20 hours of classroom training. Bank employees who are authorized to sell additional investment products and securities should receive training that is appropriate to pass the NYSE's series 7 general securities representative examination, which typically involves 160 to 250 hours of study, including at least 40 hours of classroom training.

The training of third-party or dual employees is the responsibility of the third party. When entering into an agreement with a third party, bank management should be satisfied that the third party is able to train third-party and dual employees with respect to compliance with the minimum disclosures and other requirements of the interagency statement. Copies of third-party training and compliance materials should be obtained and reviewed by the bank to monitor the third party's performance regarding its training obligations.

Training of Bank Personnel Who Make Referrals

Bank employees, such as tellers and platform personnel, who are not authorized to provide investment advice, make investment recommendations, or sell nondeposit investment products, but who may refer customers to authorized nondeposit investment products sales personnel, should receive training about the strict limitations on their activities. In general, bank personnel who are not authorized to sell nondeposit investment products are not permitted to discuss general or specific investment products, prequalify prospective customers as to financial status and investment history and objectives, open new accounts, or take orders on a solicited or unsolicited basis. These personnel may contact customers for the purposes of—

- determining whether the customer wishes to receive investment information
- inquiring whether the customer wishes to discuss investments with an authorized sales representative, and
- arranging appointments to meet with authorized bank sales personnel or third-party broker-dealer registered sales personnel.

The minimum disclosure guidelines do not apply to referrals made by personnel not authorized to sell nondeposit investment products if the referral does not provide investment advice, identify specific investment products, or make investment recommendations.

Supervision of Personnel

Bank policies and procedures should designate, by title or name, the individuals responsible for supervising nondeposit investment product sales activities, as well as the referral activities of bank employees not authorized to sell these products. Personnel responsible for managing

the sales programs for these products should have supervisory experience and training equivalent to that required of a general securities principal, as required by the NASD for broker-dealers. Supervisory personnel should be responsible for the bank's compliance with policies and procedures on nondeposit investment products, applicable laws and regulations, and the interagency statement. When sales of these products are conducted by a third party, supervisory personnel should be responsible for monitoring compliance with the agreement between the bank and the third party, as well as compliance with the interagency statement, particularly the guideline calling for nondeposit investment product sales to be separate and distinct from the deposit activities of the bank.

SUITABILITY AND SALES PRACTICES

Suitability of Recommendations

Suitability refers to the matching of customer financial means and investment objectives with a suitable product. If customers are placed into unsuitable investments, the resulting loss of consumer confidence could have detrimental effects on the bank's reputation. Many first-time investors may not fully understand the risks associated with nondeposit investment products and may assume that the bank is responsible for the preservation of the principal of their investment.

Banks that sell nondeposit investment products directly to customers should develop detailed policies and procedures addressing the suitability of investment recommendations and related recordkeeping requirements. Sales personnel that recommend nondeposit investment products to customers should have reasonable grounds for believing that the recommended products are suitable for the particular customer on the basis of information he or she has provided. A reasonable effort must be made to obtain, record, and update information concerning the customer's financial profile (for example, tax status, other investments, income), investment objectives, and other information necessary to make recommendations.

In determining whether sales personnel are meeting their suitability responsibilities, examiners should review the practices for conformance with the bank's policies and procedures. The examiner's review should include a sample of customer files to determine the extent of customer information collected, recorded, and updated (for subsequent purchases) and should determine whether investment recommendations appear unsuitable in light of this information.

Nondeposit investment product sales programs conducted by third-party broker-dealers are subject to the NASD's suitability and other sales practice rules. To avoid duplicating NASD examination efforts, examiners should rely on the NASD's most recent sales practice review of the third party, when available. If an NASD review has not been completed within the last two years, Reserve Banks should consult with Board staff to determine an appropriate examination scope for suitability compliance before proceeding further.

Sales Practices and Customer Complaints

Banks should have policies and procedures that address undesirable practices by sales personnel, such as practices to generate additional commission income for the employee by churning or switching accounts from one product to another. Banks should have policies and procedures for handling customer complaints related to nondeposit investment products. The process should provide for the recording and tracking of all complaints and require periodic reviews of complaints by compliance personnel. The merits and circumstances of each complaint (including all documentation relating to the transaction) should be considered when determining the proper form of resolution. Reasonable timeframes should be established for addressing complaints.

COMPENSATION

Incentive compensation programs specifically related to the sale of nondeposit investment products may include sales commissions, limited fees for referring prospective customers to an authorized sales representative, and nonmonetary compensation (prizes, awards, and gifts). Compensation that is paid by unaffiliated third parties (for example, mutual fund distributors) to bank staff must be approved in writing by

bank management, be consistent with the bank's written internal code of conduct for the acceptance of remuneration from third parties, and be consistent with the proscriptions of the Bank Bribery Act (18 USC 215) and the banking agencies' implementing guidelines to that act. Compensation policies should establish appropriate limits on the extent of compensation that may be paid to banking organization staff by unaffiliated third parties.

Incentive compensation programs must not be structured in such a way that they result in unsuitable investment recommendations or sales to customers. In addition, if sales personnel sell both deposit and nondeposit products, similar financial incentives should be in place for sales of both types of products. A compensation program that offers significantly higher remuneration for selling a specific product (such as a proprietary mutual fund) may be inappropriate if it results in unsuitable recommendations to customers. A compensation program that is intended to provide remuneration for a group of bank employees (such as a branch or department) is permissible as long as the program is based on the group's overall performance in meeting bank objectives for a broad variety of bank services and products and not on the volume of sales of nondeposit investment products.

Individual bank employees, such as tellers, may receive a one-time nominal fee of a fixed-dollar amount for referring customers to authorized sales personnel to discuss nondeposit investment products. However, the payment of the fee should not depend on whether the referral results in a transaction. Nonmonetary compensation to bank employees for referrals should be similarly structured. Auditors and compliance personnel should not participate in incentive compensation programs that are directly related to the results of nondeposit investment product sales programs.

COMPLIANCE

Banks must develop and maintain written policies and procedures that effectively monitor and assess compliance with the interagency statement and other applicable laws and regulations and that ensure appropriate follow-up to correct identified deficiencies. Compliance programs should be independent of sales activities with respect to scheduling, compensation, and performance evaluations. Compliance findings should periodically be reported to the bank's board of directors or a designated committee of the board as part of the institution's ongoing oversight of nondeposit investment product activities. Compliance personnel should have appropriate training and experience with nondeposit investment product sales programs, applicable laws and regulations, and the interagency statement.

Banks should institute compliance programs for nondeposit investment products that are similar to those of securities broker-dealers. This includes a review of new accounts and a periodic review of transactions in existing accounts to identify any potentially abusive practices, such as unsuitable recommendations, churning, or switching. Compliance personnel should also oversee the prompt resolution of customer complaints and review complaint logs for questionable sales practices. Management-information-system reports on early redemptions and sales patterns for specific sales representatives and products should also be used by compliance personnel to identify any potentially abusive practices. In addition, the referral activities of bank personnel should be reviewed to ensure that they conform to the guidelines in the interagency statement.

When nondeposit investment products are sold by third parties on bank premises, the bank's compliance program should provide for oversight of the third party's compliance with its agreement with the bank, including its conformance to the disclosure and separate-facilities guidelines of the interagency statement. The results of this oversight should be reported to the board of directors or a designated committee of the board. Management should obtain the third party's commitment to promptly correct identified problems. Proper follow-up by the bank's compliance personnel should verify the third party's corrective actions.

AUDITS

Audit personnel should be responsible for assessing the effectiveness of the institution's compliance function and overall management of the nondeposit investment product sales program. The scope and frequency of audit reviews of nondeposit investment product activities will depend on the complexity and sales volume of a

sales program and on whether there are any indications of potential or actual problems. Audits should cover all of the issues discussed in the interagency statement. Internal audit staff should be familiar with nondeposit investment products and receive ongoing training. Findings should be reported to the board of directors or to a designated committee of the board, and proper follow-up should be performed. Audit activities with respect to third parties should include a review of their compliance function and the effectiveness of the bank's oversight of the third party's activities.

1. To determine that the banking organization has taken appropriate measures to ensure that retail customers clearly understand the differences between insured deposits and nondeposit investment products and that they receive the minimum disclosures both orally during sales presentations (including telemarketing) and in writing.
2. To assess the adequacy of the institution's policies and procedures, sales practices, and oversight by management and the board of directors to ensure an operating environment that fosters customer protection in all facets of the sales program.
3. To ensure that the sales program is conducted in a safe and sound manner that is in compliance with the interagency statement, Federal Reserve guidelines, regulations, and applicable laws.
4. To assess the effectiveness of the institution's compliance and audit programs for nondeposit investment product operations.
5. To obtain commitments for corrective action when policies, procedures, practices, or management oversight is deficient or when the institution has failed to comply with the interagency statement or applicable laws and regulations.

1. Verify through the minutes of the board of directors that the directors have approved the sale of uninsured annuities, reviewed, and approved the choice of an underwriter in the past year.
2. Determine if the bank adequately evaluates the underwriter's financial condition at least annually and regularly reviews the credit ratings assigned to the underwriter by at least two independent agencies evaluating annuity underwriters. (Banks engaged in the sale of annuities are expected to sell only products of financially secure underwriters and to make current ratings of the underwriter available to an investor when purchasing an uninsured annuity.)
3. Verify that the bank does not sell uninsured annuities at teller windows or other areas where retail deposits are routinely accepted.
4. Assess the adequacy of disclosures and the separation of the marketing and sale of uninsured annuities from the retail deposit-taking function by ensuring that—
   a. the contract, advertising, and all related documents disclose prominently in bold print that the annuities are not deposits or obligations of an insured depository institution and are not insured by the Federal Deposit Insurance Corporation;
   b. advertisements do not contain words, such as "deposit," "CD," etc., that could lead an investor to believe an annuity is an insured deposit instrument;
   c. the obligor of the annuity contract is prominently disclosed and names or logos of the insured bank are not used in a way that might suggest the insured bank is the obligor;
   d. adequate verbal disclosures are made during telemarketing contacts and at the time of sale;
   e. retail deposit-taking employees of the insured depository institution are not engaged in the promotion or sale of uninsured annuities;
   f. information on uninsured annuities is not contained in retail deposit statements of customers (either as advertising on deposit statements or as "junk mail" stuffers included with deposit statements) or in the immediate retail deposit-taking area;
   g. account information on annuities owned by customers is not included on insured deposit statements; and
   h. officer or employee remuneration associated with selling annuities is limited to reasonable levels in relation to the individual's salary. (As a guideline in reviewing remuneration, see the Board's policy statement on disposition of credit life insurance, as discussed in the Consumer Credit, Examination Procedures, section of this manual.)
5. If the bank allows a third-party entity to market annuities on depository-institution premises, assess the adequacy of disclosures and the separation of the marketing and sale of uninsured annuities from the retail deposit-taking function by determining that—
   a. the bank has ensured that the third-party company is properly registered or licensed to conduct this activity,
   b. bank personnel are not involved in sales activities conducted by the third party,
   c. desks or offices used to market or sell annuities are separate and distinctly identified as being used by an outside party, and
   d. bank personnel do not normally use desks or offices used by a third party for annuities sales.
6. Encourage the bank to obtain a signed statement from the customer indicating that the customer understands that the annuity is not a deposit or any other obligation of the bank, that the bank is only acting as an agent for the insurance company (underwriter), and that the annuity is not FDIC-insured.

Fiduciary activities and other related services generally include traditional trust services, such as personal trust, corporate trust, and transfer-agent services and employee benefit account products and services, as well as custody and securities-lending services, clearing and settlement, private banking, asset management, and investment advisory activities. (See SR-01-5.)

Pursuant to 12 USC 24 (seventh), 92a, and 93a, the Office of the Comptroller of the Currency (OCC) has established standards (the OCC rules for fiduciary activities of national banks). These rules are typically considered the industry standard for fiduciary activities of all financial institutions operating in the United States. (See 12 CFR 9.) When considering whether a state member bank has adhered to industry standards for fiduciary activities, Federal Reserve System (FRS) examiners can refer to the guidance set forth in the OCC rules and FRS and OCC examination manuals, as well as the examination materials issued by other U.S. financial institution regulatory agencies. With respect to a state member bank subsidiary, the appropriate bank, thrift, or functional regulator has the primary supervisory responsibility for evaluating risks, hedging, and risk management at the legal-entity level for the entity that the regulator supervises. (See SR-00-13.) Examiners should seek to use the examination findings of the functional regulator.

A risk-focused fiduciary examination concentrates on understanding and evaluating risk and assessing the internal controls the state member bank has employed to manage risk. The program encompasses continuous monitoring; targeted reviews of fiduciary activities; preparation of supervisory risk profiles and assessments; and the development of supervisory plans, which are integrated into the preplanning of an examination. Conclusions are used to develop an overall safety-and-soundness evaluation of the state member bank's fiduciary activities. (See SR-96-10.)

The Federal Reserve System's fiduciary-examination program reviews and assesses the risk-management practices and related aspects of a state member bank's fiduciary activities. This approach results in (1) the use of a more diversified examiner population, including those with capital-markets, information systems, and safety-and-soundness experience; (2) an emphasis on assessing the individual organization's unique risk profile; and (3) reviews of risk identification, measurement, monitoring, and control. Examiners should use the state member bank's control disciplines (internal audit, risk management, and compliance program) whenever possible.

Examiners have access to a broad variety of FRS supervisory information and analytical support tools to evaluate the fiduciary activities of financial institutions. The Uniform Bank Performance Report (UBPR) can assist examiners in evaluating a state member bank's fiduciary business lines or activities relative to its peers. (See the UBPR, pages Trust 1 and Trust 1A.) Beginning with the December 2002 release, ''Section II: Technical Information'' of the *UBPR User's Guide* (available online at www.ffiec.gov/ubprguide.htm) discusses the availability of the Total Fiduciary Assets within a fiduciary group number (peer group). (See page II-3.) ''Total Fiduciary Assets'' are the totals of managed and nonmanaged fiduciary assets for FDIC-insured commercial and savings banks, as reported on Schedule RC-T of the call report.

COMPLEX FIDUCIARY ORGANIZATIONS

SR-01-5 explains that complex fiduciary organizations are those banking organizations that conduct significant or complex fiduciary activities. This includes large complex banking organizations (LCBOs), other large or regional institutions for which fiduciary activities represent a significant portion of their business, and clearing agencies registered with the Securities and Exchange Commission (SEC) for which the Federal Reserve is the primary supervisor. The fiduciary-examination frequency should be determined on the basis of the impact that fiduciary activities have on the organization's risk profile. At a minimum, all material fiduciary business lines should be subject to examination over a two-year period or examination cycle as part of the continuous supervision process, with higher-risk areas generally reviewed annually.

Composite Uniform Interagency Trust Rating System (UITRS) ratings and transfer-agent ratings reflecting the overall condition of the fiduciary function at each institution, and any component ratings considered relevant, should be

assigned or updated in a timely manner on the basis of the results of examinations, targeted reviews, or other assessments of fiduciary activities. UITRS ratings do not need to be assigned for each targeted business-line review. However, at a minimum, composite UITRS and transfer-agent ratings should be updated annually, and any material findings related to these areas should be included in the annual summary supervisory report. Any significant concerns should be reflected in the safety-and-soundness examination ratings. Fiduciary risks and fiduciary-risk management assessments should also be reflected in the relevant risk-assessment and risk-management ratings for the banking organization, as necessary.

OTHER INSTITUTIONS OFFERING FIDUCIARY AND TRANSFER-AGENT SERVICES

The frequency of fiduciary and transfer-agent examinations for other institutions, generally smaller state-chartered Federal Reserve member banks and trust companies with noncomplex operations, should be determined on the basis of the significance of their fiduciary and transfer-agent activities and an assessment of the level of risk the activities present to the institution. This scheduling guidance also applies to initial examinations of new institutions and to those institutions subject to Federal Reserve supervision as a result of a charter conversion.

At a minimum, fiduciary activities should be reviewed no less frequently than during every other routine safety-and-soundness examination. Examinations governed by alternating examination programs with state banking authorities may continue to be performed in accordance with those arrangements or as necessary to incorporate the provisions of SR-01-5. Examinations of fiduciary activities at noncomplex limited-purpose trust companies and other fiduciary institutions subject to supervision by the Federal Reserve that do not receive routine safety-and-soundness examinations should be conducted no less frequently than every two years.

Composite UITRS and transfer-agent examination ratings reflecting the overall condition of the function, and any component ratings considered relevant, should be assigned or updated at the completion of the examination or assessment. Material examination findings should be integrated into the overall examination report for the institution, which should clearly indicate the significance of any findings to the safety and soundness of the institution and the impact of the findings on any relevant risk assessments and risk-management ratings.

ORGANIZATIONS WITH SUPERVISORY CONCERNS

Organizations whose fiduciary activities have raised supervisory concerns should be subject to an additional level of supervisory attention on the basis of the severity of those supervisory concerns. Generally, this would include those organizations with a composite UITRS rating of 3, 4, or 5; a transfer-agent rating of B or C; or significant deficiencies in one or more component-rating categories. In the case of an institution assigned a UITRS rating of 4 or 5 or a transfer-agent rating of C, supervisory action should be initiated promptly and continued until the problems or deficiencies have been appropriately addressed.

Under the Securities and Exchange Act of 1934, the Federal Reserve continues to be responsible for examining transfer agents and clearing agencies for which it is the primary supervisor, including reviewing compliance with SEC rules. Any material violations of transfer-agent or clearing-agency rules must be reported promptly to Board staff to facilitate coordination with the SEC.

RISK PROFILE OF FIDUCIARY ACTIVITIES

Regular supervisory assessments of the risk of fiduciary activities, as outlined in SR-01-5, support the supervisory process. Risk profiles for LCBOs are updated quarterly. These risk profiles should include explicit consideration of the risks of fiduciary activities. For other complex fiduciary organizations, risk profiles reflecting fiduciary activities should be prepared and updated as needed, but no less frequently than annually. For these organizations, supervisory plans should detail the fiduciary specialist's recommended examination coverage of fiduciary activities. For banking organizations

supervised by the Federal Reserve that have smaller, noncomplex fiduciary operations, formal risk profiles may not be necessary. However, fiduciary-risk information should normally be updated at each examination or inspection and incorporated into supervisory plans.

Risk profiles should include an assessment of the inherent risk in the organization's fiduciary activities, as well as a consideration of the effectiveness of its risk management. Risk assessments would normally include the following factors:

- the size and number of fiduciary accounts and assets administered
- the nature and complexity of fiduciary products and services offered
- significant changes to management or staffing for fiduciary services
- significant changes to data processing systems supporting fiduciary services
- new affiliations, partnerships, or outsourcing arrangements
- changes in strategic direction affecting fiduciary services or exposure to emerging risks
- significant litigation, settlements, or charge-offs
- the length of time since the last on-site examination in which fiduciary activities were reviewed, and the scope of that examination
- the significance of prior examination findings
- the effectiveness of the organization's control environment, including its audit function, and the adequacy of its risk-management practices relative to the nature and scope of its business

RISK FOCUS

As explained in SR-96-10, for a complex institution, fiduciary examiners will direct their attention to assessing the organization's func-

tions and its ability to identify, measure, monitor, and control fiduciary, market, credit, and operational risks. Examiners should assess risks that result from the fiduciary's investment-management, investment advisory, mutual funds, global custody, and securities-lending and processing activities. Any other activities that are subject to adverse movements in market rates or prices, or to operating problems associated with processing a large volume of securities, should also be assessed. These fiduciary activities could result in material losses to trust customers and, in turn, expose the institution to financial losses and litigation if not conducted in a manner consistent with the fiduciary's duty of loyalty and the investor's stated objectives.

A review of internal controls and policies and procedures is an integral part of the examination program. Facets of a fiduciary examination include management competence and accountability, management's review of risks associated with the introduction of new products and services, and management's overall risk awareness.

The emphasis on risk assessment and control parallels the guidelines and procedures pertaining to state member bank examinations and bank holding company inspections, as described in SR-95-51 and SR-16-11, and recognizes the efforts of many progressive institutions in establishing fiduciary-risk assessment and control initiatives of their own. When rating the quality of risk management of fiduciary activities, examiners should place primary consideration on findings relating to the following elements of a sound risk-management system: (1) active board and senior management oversight; (2) adequate policies, procedures, and limits; (3) adequate risk-measurement, -monitoring, and management information systems; and (4) comprehensive internal controls. Each of these elements is described further below, along with a list of considerations relevant to assessing the adequacy of each element.

Active Board and Management Oversight

Given that a board of directors has ultimate responsibility for all of the activities of its institution, the board should approve overall fiduciary business strategies and policies, including those related to identifying, measuring, monitoring, and controlling fiduciary risks. A board of directors must understand the nature of the risks that are significant to the organization, and it should ensure that management is taking the steps necessary to manage these risks.

Senior management has the responsibility for implementing approved strategies in a way that will limit fiduciary risks and ensure compliance with laws and regulations. Senior management should, therefore, be fully involved in the fiduciary activities of their institution and have sufficient knowledge of all fiduciary business lines to ensure that necessary policies, controls, and risk-monitoring systems are in place and that accountability and lines of authority are clearly defined. In assessing the quality of fiduciary oversight by boards of directors and senior management, examiners should consider whether these conditions exist:

- The board and senior management have a clear understanding and working knowledge of the types of fiduciary activities the institution performs and of the risks inherent in them. They have approved appropriate policies, procedures, recordkeeping systems, and reporting systems to support the fiduciary activities and to help measure and monitor risks. They have established procedures to stay informed about changes in fiduciary activities and the associated risks.
- Management at all levels adequately supervises the daily activities of officers and employees to ensure that the lines of fiduciary business are managed and staffed by persons whose knowledge, experience, and expertise are consistent with the nature and scope of the organization's fiduciary activities.
- Before offering new services or introducing new products, management identifies the fiduciary risks associated with them and ensures that internal controls are in place to manage the service or product and its accompanying risk.

Adequate Policies, Procedures, and Limits

An institution's directors and senior management should establish fiduciary and fiduciary-risk management policies and procedures commensurate with the types of activities the institution conducts. The policies and procedures should provide enough detailed guidance to ensure that all material areas of fiduciary

activity and risk are addressed. They should also be modified when necessary to respond to changes in the organization's activities. A smaller, less complex institution that has effective management and that is heavily involved in daily operations generally would be expected to have more basic policies addressing the significant areas of its activities and setting forth a limited but appropriate set of requirements and procedures. In a larger institution, where senior management must rely on a widely dispersed staff to implement strategies in a wide range of complex situations, far more detailed policies and related procedures would be expected. In assessing the adequacy of an institution's fiduciary and fiduciary-risk management policies and procedures, examiners should consider whether these conditions exist:

- The institution's policies and procedures adequately address the fiduciary activities performed and are consistent with management's experience level and with the institution's stated goals and objectives.
- The institution's policies and procedures provide for adequate identification, measurement, monitoring, and control of the risks posed by its fiduciary activities.
- Policies clearly establish accountability and set forth lines of authority.
- Policies provide for review of new fiduciary services and activities to ensure that they are suitable and consistent with fiduciary-customer objectives, and to ensure that the systems necessary to identify, measure, monitor, and control risks associated with new services and activities are in place before the activity is initiated.

Adequate Risk-Monitoring and Management Information Systems

Risk monitoring requires institutions to identify and measure all areas of material fiduciary risk continuously. Risk-monitoring activities must be supported by management information systems that provide senior management with timely reports on financial condition, operating performance, marketing efforts, new products and services, pending or threatened litigation, and risk exposure arising from fiduciary activities. The information system also must provide regular and more detailed reports for managers engaged in the daily management of the institution's activities.

The sophistication of risk-monitoring and control information systems should be commensurate with the complexity of the institution's fiduciary operations. Less complex institutions may require only a limited number of management reports to support risk-monitoring activities. Larger, more complex institutions, however, would be expected to have much more comprehensive reporting and monitoring systems. These systems would allow for more frequent reporting and closer monitoring of complex activities. In assessing the adequacy of an institution's measurement and monitoring of fiduciary risk, examiners should consider whether these conditions exist:

- The institution's fiduciary-risk monitoring practices and reports encompass all of its business lines and activities, and they are structured to monitor exposures consistent with established goals, limits, and objectives.
- Key assumptions, data sources, and procedures used in identifying, measuring, and monitoring fiduciary risk are appropriate for the activities the institution performs and are adequately documented and continuously tested for reliability.
- Reports to management are accurate and timely and contain sufficient information for policy and decision makers to identify any adverse trends and any potential or real problems. The reports must be adequate for management to evaluate the level of fiduciary risk faced by the institution.

Adequate Internal Controls

A comprehensive internal-control structure is critical to the safe and sound functioning of an institution and its fiduciary-risk management system. Establishing and maintaining a system of internal controls that sets forth official lines of authority and an appropriate segregation of duties is one of management's most important responsibilities.

A well-structured system of internal controls promotes effective fiduciary operations and reliable reporting; safeguards assets; and helps to ensure compliance with laws, regulations, and institutional policies. Controls should be periodically tested by an independent party (prefer-

ably the auditor or at least an individual not involved in the process being reviewed) who reports directly to either the institution's board of directors or one of its designated committees. Given the importance of appropriate internal controls to organizations of all sizes and risk profiles, the results of these reviews should be adequately documented, as should management's responses to them. In evaluating the adequacy of an institution's internal controls as they relate to fiduciary activities, examiners should consider whether these conditions exist:

- The system of internal controls is appropriate to the type and level of fiduciary activities.
- The institution's organizational structure establishes clear lines of authority and responsibility.
- Reporting lines are sufficiently independent of the control areas and from the business lines, and there is adequate separation of duties throughout the institution.
- Financial, operational, and regulatory reports are reliable, accurate, and timely.
- Adequate procedures exist for ensuring compliance with laws and regulations.
- Internal-audit or other control-review practices provide for independence and objectivity.
- Internal controls and information systems are adequately tested and reviewed, with findings documented and weaknesses given appropriate and timely attention.
- The board of directors or the audit committee reviews the effectiveness of internal audits and other control-review activities regularly.

The fiduciary-risk assessment and control categories and tools listed above are not all-inclusive. They are guidelines for the fiduciary examiner and fiduciary-activities management to use in their risk-assessment and -control efforts. The examination of fiduciary activities may require some modification, depending on how the activities are organized and the complexity of the products and services offered.

INVESTMENT OF FIDUCIARY ASSETS IN MUTUAL FUNDS AND POTENTIAL CONFLICTS OF INTEREST

Banks and trust institutions encounter various direct or indirect financial incentives to place trust assets with particular mutual funds. These incentives include fees for using nonaffiliated fund families as well as incentives for using an institution's proprietary mutual funds. The primary supervisory concern is that an institution may fail to act in the best interest of its beneficiaries if it stands to benefit independently from a particular investment. As a result, an institution may be exposed to an increased risk of legal action by account beneficiaries, and it could potentially violate laws or regulations. The Federal Reserve Board issued SR-99-7 to help institutions minimize these risks and ensure that their activities meet fiduciary standards.

Institutions should ensure that they perform and document an appropriate level of due diligence before entering into any compensation arrangements with mutual fund providers or before placing fiduciary assets in their own proprietary mutual funds. SR-99-7 discusses the type of measures that should be included in this process, including a reasoned legal opinion addressing the activity, appropriate policies and procedures, and documented analysis and ongoing review of investment decisions. For issues pertaining to retail sales of nondeposit investment products and matters relating to compensation, see section 4170.1.

Types of Financial Incentives

Financial incentives for placing trust assets with particular mutual funds range from payments structured as reimbursements for services or for transferring business to an unaffiliated fund family, to financial benefits that arise from using mutual funds that are managed by the institution or an affiliate. In some cases, such as service fees for administrative and recordkeeping functions performed by the trust institution, the permissibility of such payments may be specifically addressed under state law. However, guidance under applicable law may be less clear for other financial incentives. In all cases, decisions to place fiduciary assets in particular investments must be consistent with the underlying trust documents and must be undertaken in the best interest of the trust beneficiary.

Certain mutual fund providers offer compensation in the form of "service" fees to institutions that invest fiduciary assets in particular mutual funds. These fees, referred to variously as shareholder, subaccounting, or administrative-

service fees, are structured as payments to reimburse the institution for performing standard recordkeeping and accounting functions for the institution's fiduciary accounts, such as maintaining shareholder subaccounts and records, transmitting mutual fund communications as necessary, and arranging mutual fund transactions. These fees are typically based on a percentage or basis-point amount of the dollar value of assets invested or on transaction volume.

Nearly every state legislature modified its laws in the 1990s to allow explicitly the acceptance of such service fees by fiduciaries under certain conditions. These conditions often include compliance with standards of prudence, quality, and appropriateness for the account, and a determination of the "reasonableness" of the fees received by the institution. The Office of the Comptroller of the Currency (OCC) also adopted these general standards for national banks.[1] However, the Employee Retirement Income Security Act of 1974 (ERISA) generally prohibits fee arrangements between fiduciaries and third parties, such as mutual fund providers, with limited exceptions.[2] ERISA requirements supersede state laws and guidelines put forth by the bank regulatory agencies.

Although there has been no comprehensive review of the extent to which mutual fund providers are offering the types of incentive payments cited above, the practice is not uncommon. In addition to these service fees, another form of compensation reportedly offered by some mutual fund providers is a lump-sum payment based on assets transferred into a mutual fund.

Similar conflict-of-interest concerns are raised by the investment of fiduciary-account assets in mutual funds for which the institution or an affiliate acts as investment adviser (referred to as "proprietary" funds). In this case, the institution receives a financial benefit from management fees generated by the mutual fund investments.[3]

Due-Diligence Measures

Although many state laws explicitly authorize certain fee arrangements in conjunction with the investment of trust assets in mutual funds, institutions nonetheless face heightened legal and compliance risks from activities in which a conflict of interest exists, particularly if proper fiduciary standards are not observed and documented. Section 23B of the Federal Reserve Act (FRA) requires, before a member bank purchases shares issued by an affiliate, including investment-fund shares, that the board of directors approve the purchase based on a determination that the purchase is a sound investment for the bank, irrespective that an affiliate is the principal underwriter.[4] Even for investments in which the institution does not exercise investment discretion, disclosure or other requirements may apply. Therefore, institutions should ensure that they perform and document an appropriate level of due diligence before entering into any fee arrangements similar to those described above or before placing fiduciary assets in proprietary mutual funds. According to SR-99-7, the following measures should be included in this process:

- *A reasoned legal opinion.* The institution should obtain a reasoned opinion of counsel that addresses the conflict of interest inherent in the receipt of fees or other forms of compensation from mutual fund providers in connection with the investment of fiduciary assets. The opinion should address the permissibility of the investment and compensation under applicable state or federal laws, the trust instrument, or court order, as well as any applicable disclosure requirements or "reasonableness" standard for fees set forth in the law.
- *Establishment of policies and procedures.* The institution should establish written policies and procedures governing the acceptance of fees or other compensation from mutual fund providers, as well as the use of proprietary mutual funds. The policies must be reviewed and approved by the institution's board of directors or its designated committee. Policies

1. In general, national banks may make these investments and receive such fees if the practice is authorized by applicable law and if the investment is prudent and appropriate for fiduciary accounts and consistent with fiduciary requirements established by state law. These requirements include a "reasonableness" test for any fees received by the institution. (OCC Interpretive Letter No. 704, February 1996.)

2. ERISA section 406(b)(3), Department of Labor, Pension Welfare and Benefits Administration Advisory Opinion 97-15A and Advisory Opinion 97-16A.

3. A Board interpretation of Federal Reserve Regulation Y addresses the investment of fiduciary-account assets in mutual funds for which the trustee bank's holding company acts as investment adviser. In general, such investments are prohibited unless specifically authorized by the trust instrument, court order, or state law. See *Federal Reserve Regulatory Service* 4–177.

4. 12 USC 371c-1(b)(2).

and procedures should, at a minimum, address the following issues: (1) designation of decision-making authority; (2) analysis and documentation of investment decisions; (3) compliance with applicable laws, regulations, and sound fiduciary principles, including any disclosure requirements or reasonableness standards for fees; and (4) staff training and methods for monitoring compliance with policies and procedures by internal or external audit staff.

- *Analysis and documentation of investment decisions.* Where an institution receives fees or other compensation in connection with fiduciary-account investments over which it has investment discretion or where such investments are made in the institution's proprietary mutual funds, the institution should fully document its analysis supporting the investment decision. This analysis should be performed on a regular, ongoing basis and would typically include factors such as historical performance comparisons to similar mutual funds, management fees and expense ratios, and ratings by recognized mutual-fund rating services. The institution should also document its assessment that the investment is, and continues to be, appropriate for the individual account, in the best interest of account beneficiaries, and in compliance with section 23B of the FRA and with provisions of the "prudent-investor" or "prudent-man rules," as appropriate.

UNIFORM INTERAGENCY TRUST RATING SYSTEM

In December 1998, the Federal Reserve Board issued implementing guidelines for the Uniform Interagency Trust Rating System (UITRS).[5] The revised UITRS was made effective for examinations commencing on or after January 1, 1999.[6] Federal Reserve examiners should assign UITRS ratings in conformance with the definitions adopted by the Federal Financial Institutions Examination Council (FFIEC), as augmented by the guidance below.

A full composite UITRS rating is *required* to be assigned as a result of all trust examinations, except for targeted examinations, where component ratings need only be assigned for those areas included within the examination's scope. In those cases, component ratings should be assigned as the targeted examinations are completed. When an institution's trust activities are examined as a series of limited reviews over a period of time, the full UITRS rating should be assigned when the examination is considered complete, or at least as often as required under SR-01-05.

Additional Considerations for Specific UITRS Components

Management

The revised UITRS puts greater emphasis on assessing the quality of an institution's risk management, consistent with guidance previously provided to Federal Reserve examiners in SR-96-10. Examiners should continue to include in risk profiles and risk-management assessments the key risks outlined in SR-95-51, including reputation risk, operational risk, legal risk, credit risk, market risk, and liquidity risk. See also SR-16-11. Whether all of these risks or a subset of them is relevant to the assessment of risk management, and thus to the management rating, depends on the scope of the particular institution's fiduciary activities. The other four UITRS rating components may also include consideration of the institution's ability to manage some or all of these risks.

Earnings

Examiners must *evaluate* earnings for all institutions that exercise fiduciary powers. In addition, an earnings *rating* must be assigned for institutions that, at the time of the examination, have total fiduciary assets of more than $100 million and for all nondeposit trust companies. For all other institutions, examiners are not required to assign a rating and should only do so in cases where fiduciary activities are significant and the earnings rating would be meaningful to the overall rating. In these cases, examiners should use the standard earnings-rating definition, rather than the alternate-rating definitions provided in the UITRS. For examinations where no earnings

5. The UITRS was developed by the Federal Financial Institutions Examination Council. SR-98-37 mandated the use of UITRS for Federal Reserve examinations of fiduciary activities.

6. See 63 *Fed. Reg.* 54704 (October 13, 1998).

rating is assigned, a rating of 0 should be given for the earnings component, and this component should be excluded from consideration in the composite rating.

Earnings ratings of 3 or worse should be reserved for institutions whose earnings performance indicates a supervisory problem requiring corrective action, which, if left unaddressed, may pose a risk to the institution. Federal Reserve examiners may, therefore, assign an earnings rating of 2 for an institution that has experienced losses in its fiduciary activities, provided that (1) management has determined that there are benefits to the overall institution or its community from offering fiduciary services, (2) losses from fiduciary activities are stable and consistent with management expectations, and (3) such losses do not have a significant adverse effect on the profitability of the institution as a whole.

Asset Management

As noted in the UITRS, the asset-management component may not be applicable for some institutions because their activities do not involve the management of discretionary assets. A rating for asset management may, therefore, be omitted for examinations of institutions whose operations are limited to activities such as directed-agency relationships, securities clearing, nonfiduciary custody relationships, or transfer-agent or registrar activities. However, this component rating should be assigned for an institution that provides investment advice, even though it does not have discretion over the account assets. Where an asset-management rating is not assigned for a particular examination, a rating of 0 should be given, and this component should be excluded from consideration in the composite rating.

Examination Reports

SR-96-26 requires that the UITRS rating be disclosed to the institution in the summary section of each examination report. In addition, the individual numerical component ratings, which should also be disclosed in the open section of the report, may be included in the summary section. If the component ratings are included in the summary section, the ratings should also be included in the open-section pages of the report in which trust findings are presented. If the Reserve Bank prefers not to disclose the examiner's evaluation of the component ratings to the institution, this information may be included in the confidential section of the report. Regardless of where in the report it appears, the evaluation must include sufficient detail to justify the rating assigned.

UITRS Description

Under the UITRS, the fiduciary activities of financial institutions are assigned a composite rating based on an evaluation and rating of five essential components of an institution's fiduciary activities. Composite and component ratings are assigned based on a 1-to-5 numerical scale. A 1 is the highest rating and indicates the strongest performance and risk-management practices and the least degree of supervisory concern. A 5 is the lowest rating and indicates the weakest performance and risk-management practices and, therefore, the highest degree of supervisory concern. The evaluation of the composite and components considers the size and sophistication, the nature and complexity, and the risk profile of the institution's fiduciary activities.

The composite rating generally bears a close relationship to the component ratings assigned. However, the composite rating is not derived by computing an arithmetic average of the component ratings. Each component rating is based on a qualitative analysis of the factors that make up a particular component and on its interrelationship with the other components. When assigning a composite rating, some components may be given more weight than others depending on the situation at the institution. In general, the assignment of a composite rating may incorporate any factor that bears significantly on the overall administration of the financial institution's fiduciary activities. Assigned composite and component ratings are disclosed to the institution's board of directors and senior management.

Management's ability to respond to changing circumstances and address the risks that may arise from changing business conditions, or from the initiation of new fiduciary activities or products, is an important factor in evaluating an institution's overall fiduciary-risk profile and the level of supervisory attention warranted. For this reason, the management component is given

special consideration when assigning a composite rating.

The ability of management to identify, measure, monitor, and control the risks of its fiduciary operations is also taken into account when assigning each component rating. It is recognized, however, that appropriate management practices may vary considerably among financial institutions, depending on the size, complexity, and risk profiles of their fiduciary activities. For less complex institutions engaged solely in traditional fiduciary activities and whose directors and senior managers are actively involved in the oversight and management of day-to-day operations, relatively basic management systems and controls may be adequate. On the other hand, at more complex institutions, detailed and formal management systems and controls are needed to address a broader range of activities and to provide senior managers and directors with the information they need to supervise day-to-day activities.

All institutions are expected to properly manage their risks. For less complex institutions engaging in less risky activities, detailed or highly formalized management systems and controls are not required to receive strong or satisfactory component or composite ratings.

Composite Ratings

Composite ratings are based on a careful evaluation of how an institution conducts its fiduciary activities. The review encompasses the capability of management, the soundness of policies and practices, the quality of service rendered to the public, and the effect of fiduciary activities on the soundness of the institution. The composite ratings are defined as follows.

Composite 1

Administration of fiduciary activities is sound in every respect. Generally, all components are rated 1 or 2. Any weaknesses are minor and can be handled in a routine manner by management. The institution is in substantial compliance with fiduciary laws and regulations. Risk-management practices are strong relative to the size, complexity, and risk profile of the institution's fiduciary activities. Fiduciary activities are conducted in accordance with sound fiduciary principles and give no cause for supervisory concern.

Composite 2

Administration of fiduciary activities is fundamentally sound. Generally, no component rating should be more severe than 3. Only moderate weaknesses are present and are well within management's capabilities and willingness to correct. Fiduciary activities are conducted in substantial compliance with laws and regulations. Overall risk-management practices are satisfactory relative to the institution's size, complexity, and risk profile. There are no material supervisory concerns and, as a result, the supervisory response is informal and limited.

Composite 3

Administration of fiduciary activities exhibits some degree of supervisory concern in one or more of the component areas. A combination of weaknesses exists that may range from moderate to severe; however, the magnitude of the deficiencies generally does not cause a component to be rated more severely than 4. Management may lack the ability or willingness to effectively address weaknesses within appropriate time frames. Additionally, fiduciary activities may reveal some significant noncompliance with laws and regulations. Risk-management practices may be less than satisfactory relative to the institution's size, complexity, and risk profile. Although problems of relative significance may exist, they are not of such importance as to pose a threat to the trust beneficiaries generally or to the soundness of the institution. The institution's fiduciary activities require more-than-normal supervision and may include formal or informal enforcement actions.

Composite 4

Fiduciary activities generally exhibit unsafe and unsound practices or conditions, resulting in unsatisfactory performance. The problems range from severe to critically deficient and may be centered around inexperienced or inattentive management, weak or dangerous operating practices, or an accumulation of unsatisfactory features of lesser importance. The weaknesses and

problems are not being satisfactorily addressed or resolved by the board of directors and management. There may be significant noncompliance with laws and regulations. Risk-management practices are generally unacceptable relative to the size, complexity, and risk profile of fiduciary activities. These problems pose a threat to the account beneficiaries generally and, if left unchecked, could evolve into conditions that could cause significant losses to the institution and ultimately undermine public confidence in the institution. Close supervisory attention is required, which means, in most cases, formal enforcement action is necessary to address the problems.

Composite 5

Fiduciary activities are conducted in an extremely unsafe and unsound manner. Administration of fiduciary activities is critically deficient in numerous major respects, with problems resulting from incompetent or neglectful administration, flagrant or repeated disregard for laws and regulations, or a willful departure from sound fiduciary principles and practices. The volume and severity of problems are beyond management's ability or willingness to control or correct. Such conditions evidence a flagrant disregard for the interests of the beneficiaries and may pose a serious threat to the soundness of the institution. Continuous close supervisory attention is warranted and may include termination of the institution's fiduciary activities.

Component Ratings

The five key components used to assess an institution's fiduciary activities are (1) the capability of management; (2) the adequacy of operations, controls, and audits; (3) the quality and level of earnings; (4) compliance with governing instruments, applicable law (including self-dealing and conflicts-of-interest laws and regulations), and sound fiduciary principles; and (5) the management of fiduciary assets. Each of the component-rating descriptions is divided into three sections: a narrative description of the component, a list of the principal factors used to evaluate that component, and a description of each numerical rating for that component. Some of the evaluation factors are repeated under one or more of the other components to reinforce the interrelationship among components.

Management

The management rating reflects the capability of the board of directors and management, in their respective roles, to identify, measure, monitor, and control the risks of an institution's fiduciary activities. The rating also reflects the ability of the board of directors and management to ensure that the institution's fiduciary activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations. Directors should provide clear guidance regarding acceptable risk-exposure levels and ensure that appropriate policies, procedures, and practices are established and followed. Senior fiduciary management is responsible for developing and implementing policies, procedures, and practices that translate the board's objectives and risk limits into prudent operating standards.

Depending on the nature and scope of an institution's fiduciary activities, management practices may need to address some or all of the following risks: reputation, operating or transaction, strategic, compliance, legal, credit, market, liquidity, and other risks. Sound management practices are demonstrated by active oversight by the board of directors and management; competent personnel; adequate policies, processes, and controls that consider the size and complexity of the institution's fiduciary activities; and effective risk-monitoring and management information systems. This rating should reflect the board's and management's ability as it applies to all aspects of fiduciary activities in which the institution is involved.

The management rating is based on an assessment of the capability and performance of management and the board of directors, including, but not limited to, the following evaluation factors:

- the level and quality of oversight and support of fiduciary activities by the board of directors and management, including committee structure and adequate documentation of committee actions
- the ability of the board of directors and management, in their respective roles, to plan for and respond to risks that may arise from

changing business conditions or the introduction of new activities or products
- the adequacy of and conformance with appropriate internal policies, practices, and controls addressing the operations and risks of significant fiduciary activities
- the accuracy, timeliness, and effectiveness of management information and risk-monitoring systems appropriate for the institution's size, complexity, and fiduciary-risk profile
- the overall level of compliance with laws, regulations, and sound fiduciary principles
- responsiveness to recommendations from auditors and regulatory authorities
- strategic planning for fiduciary products and services
- the level of experience and competence of fiduciary management and staff, including issues relating to turnover and succession planning
- the adequacy of insurance coverage
- the availability of competent legal counsel
- the extent and nature of pending litigation associated with fiduciary activities, and its potential impact on earnings, capital, and the institution's reputation
- the process for identifying and responding to fiduciary-customer complaints.

Ratings of management. A rating of 1 indicates strong performance by management and the board of directors and strong risk-management practices relative to the size, complexity, and risk profile of the institution's fiduciary activities. All significant risks are consistently and effectively identified, measured, monitored, and controlled. Management and the board are proactive and have demonstrated the ability to promptly and successfully address existing and potential problems and risks.

A rating of 2 indicates satisfactory management and board performance and risk-management practices relative to the size, complexity, and risk profile of the institution's fiduciary activities. Moderate weaknesses may exist, but are not material to the sound administration of fiduciary activities and are being addressed. In general, significant risks and problems are effectively identified, measured, monitored, and controlled.

A rating of 3 indicates management and board performance that needs improvement or risk-management practices that are less than satisfactory given the nature of the institution's fiduciary activities. The capabilities of management or the board of directors may be insufficient for the size, complexity, and risk profile of the institution's fiduciary activities. Problems and significant risks may be inadequately identified, measured, monitored, or controlled.

A rating of 4 indicates deficient management and board performance or risk-management practices that are inadequate considering the size, complexity, and risk profile of the institution's fiduciary activities. The level of problems and risk exposure is excessive. Problems and significant risks are inadequately identified, measured, monitored, or controlled and require immediate action by the board and management to protect the assets of account beneficiaries and to prevent erosion of public confidence in the institution. Replacing or strengthening management or the board may be necessary.

A rating of 5 indicates critically deficient management and board performance or risk-management practices. Management and the board of directors have not demonstrated the ability to correct problems and implement appropriate risk-management practices. Problems and significant risks are inadequately identified, measured, monitored, or controlled and now threaten the continued viability of the institution or its administration of fiduciary activities, and they pose a threat to the safety of the assets of account beneficiaries. Replacing or strengthening management or the board of directors is necessary.

Operations, Internal Controls, and Auditing

The operations, internal controls, and auditing rating reflects the adequacy of the institution's fiduciary operating systems and internal controls in relation to the volume and character of business conducted. Audit coverage must ensure the integrity of the financial records, the sufficiency of internal controls, and the adequacy of the compliance process.

Fiduciary operating systems, internal controls, and the audit function subject an institution primarily to transaction and compliance risk. Other risks, including reputation, strategic, and financial risk, also may be present. The ability of management to identify, measure, monitor, and control these risks is reflected in this rating.

The operations, internal controls, and auditing rating is based on, but not limited to, an assess-

ment of the following evaluation factors:

- operations and internal controls, including the adequacy of—
  - — staff, facilities, and operating systems;
  - — records, accounting, and data processing systems (including controls over systems access and such accounting procedures as aging, investigation, and disposition of items in suspense accounts);
  - — trading functions and securities-lending activities;
  - — vault controls and securities movement;
  - — segregation of duties;
  - — controls over disbursements (checks or electronic) and unissued securities;
  - — controls over income-processing activities; and
  - — reconciliation processes (depository, cash, vault, subcustodians, suspense accounts, etc.)
- disaster or business-recovery programs—
  - — hold-mail procedures and controls over returned mail, and
  - — investigation and proper escheatment of funds in dormant accounts
- auditing, including—
  - — the independence, frequency, quality, and scope of the internal and external fiduciary-audit function relative to the volume, character, and risk profile of the institution's fiduciary activities;
  - — the volume or severity of internal-control and audit exceptions and the extent to which these issues are tracked and resolved; and
  - — the experience and competence of the audit staff.

Ratings of operations, internal controls, and auditing. A rating of 1 indicates that operations, internal controls, and auditing are strong in relation to the volume and character of the institution's fiduciary activities. All significant risks are consistently and effectively identified, measured, monitored, and controlled.

A rating of 2 indicates that operations, internal controls, and auditing are satisfactory in relation to the volume and character of the institution's fiduciary activities. Moderate weaknesses may exist, but are not material. Significant risks, in general, are effectively identified, measured, monitored, and controlled.

A rating of 3 indicates that operations, internal controls, or auditing need improvement in relation to the volume and character of the institution's fiduciary activities. One or more of these areas are less than satisfactory. Problems and significant risks may be inadequately identified, measured, monitored, or controlled.

A rating of 4 indicates deficient operations, internal controls, or audits. One or more of these areas are inadequate or the level of problems and risk exposure is excessive in relation to the volume and character of the institution's fiduciary activities. Problems and significant risks are inadequately identified, measured, monitored, or controlled and require immediate action. Institutions with this level of deficiencies may make little provision for audits, or they may evidence weak or potentially dangerous operating practices in combination with infrequent or inadequate audits.

A rating of 5 indicates critically deficient operations, internal controls, or audits. Operating practices, with or without audits, pose a serious threat to the safety of assets of fiduciary accounts. Problems and significant risks are inadequately identified, measured, monitored, or controlled and now threaten the ability of the institution to continue engaging in fiduciary activities.

Earnings

The earnings rating reflects the profitability of an institution's fiduciary activities and their effect on the financial condition of the institution. The use and adequacy of budgets and earnings projections by functions, product lines, and clients are reviewed and evaluated. Risk exposure that may lead to negative earnings is also evaluated.

An evaluation of earnings is required for all institutions with fiduciary activities. An assignment of an earnings rating, however, is required only for institutions that, at the time of the examination, have total trust assets of more than $100 million or that are a nondeposit trust company.

The evaluation of earnings is based on, but not limited to, an assessment of the following factors:

- the profitability of fiduciary activities in relation to the size and scope of those activities and to the overall business of the institution
- the overall importance to the institution of offering fiduciary services to its customers and local community

- the effectiveness of the institution's procedures for monitoring fiduciary-activity income and expense relative to the size and scope of these activities and their relative importance to the institution, including the frequency and scope of profitability reviews and planning by the institution's board of directors or a committee thereof

For those institutions for which a rating of earnings is mandatory, additional factors should include the following:

- the level and consistency of profitability, or the lack thereof, generated by the institution's fiduciary activities in relation to the volume and character of the institution's business
- dependence on nonrecurring fees and commissions, such as fees for court accounts
- the effects of charge-offs or compromise actions
- unusual features regarding the composition of business and fee schedules
- accounting practices that contain practices such as (1) unusual methods of allocating direct and indirect expenses and overhead, or (2) unusual methods of allocating fiduciary income and expense where two or more fiduciary institutions within the same holding company family share fiduciary services or processing functions
- the extent of management's use of budgets, projections, and other cost-analysis procedures
- methods used for directors' approval of financial budgets or projections
- management's attitude toward growth and new-business development
- new-business development efforts, including types of business solicited, market potential, advertising, competition, relationships with local organizations, and an evaluation by management of the risk potential inherent in new business areas

Ratings of earnings. A rating of 1 indicates strong earnings. The institution consistently earns a rate of return on its fiduciary activities that is commensurate with the risk of those activities. This rating would normally be supported by a history of consistent profitability over time and a judgment that future earnings prospects are favorable. In addition, management techniques for evaluating and monitoring earnings performance are fully adequate, and there is appropriate oversight by the institution's board of directors or a committee thereof. Management makes effective use of budgets and cost-analysis procedures. Methods used for reporting earnings information to the board of directors, or a committee thereof, are comprehensive.

A rating of 2 indicates satisfactory earnings. Although the earnings record may exhibit some weaknesses, earnings performance does not pose a risk to the overall institution nor to its ability to meet its fiduciary obligations. Generally, fiduciary earnings meet management targets and appear to be at least sustainable. Management processes for evaluating and monitoring earnings are generally sufficient in relationship to the size and risk of fiduciary activities that exist, and any deficiencies can be addressed in the normal course of business. A rating of 2 may also be assigned to institutions with a history of profitable operations if there are indications that management is engaging in activities with which it is not familiar or where there may be inordinately high levels of risk present that have not been adequately evaluated. Alternatively, an institution with otherwise strong earnings performance may also be assigned a 2 rating if there are significant deficiencies in its methods used to monitor and evaluate earnings.

A rating of 3 indicates less-than-satisfactory earnings. Earnings are not commensurate with the risk associated with the fiduciary activities undertaken. Earnings may be erratic or exhibit downward trends, and future prospects are unfavorable. This rating may also be assigned if management processes for evaluating and monitoring earnings exhibit serious deficiencies, provided the deficiencies identified do not pose an immediate danger to either the overall financial condition of the institution or its ability to meet its fiduciary obligations.

A rating of 4 indicates earnings that are seriously deficient. Fiduciary activities have a significant adverse effect on the overall income of the institution and its ability to generate adequate capital to support the continued operation of its fiduciary activities. The institution is characterized by fiduciary earnings performance that is poor historically or that faces the prospect of significant losses in the future. Management processes for monitoring and evaluating earnings may be poor. The board of directors has not adopted appropriate measures to address significant deficiencies.

A rating of 5 indicates critically deficient earnings. In general, an institution with this

rating is experiencing losses from fiduciary activities that have a significant negative impact on the overall institution, representing a distinct threat to its viability through the erosion of its capital. The board of directors has not implemented effective actions to address the situation.

Alternate rating of earnings. The UITRS alternate rating of earnings is *not* for use by Federal Reserve System examiners, per the December 1998 Federal Reserve UITRS implementing guidelines. For institutions where the assignment of an earnings rating is not required by the UITRS, an FFIEC federal supervisory agency has the option to assign an earnings rating using an alternate set of ratings. The alternate ratings are provided here so examiners will be able to interpret earnings ratings assigned by other banking supervisors that have adopted the alternate-rating system for earnings. Under the alternate-ratings scheme, alternate ratings are assigned based on the level of implementation of four minimum standards by the board of directors and management:

- *Standard No. 1.* The institution has reasonable methods for measuring income and expense commensurate with the volume and nature of the fiduciary services offered.
- *Standard No. 2.* The level of profitability is reported to the board of directors, or a committee thereof, at least annually.
- *Standard No. 3.* The board of directors periodically determines that the continued offering of fiduciary services provides an essential service to the institution's customers or to the local community.
- *Standard No. 4.* The board of directors, or a committee thereof, reviews the justification for the institution to continue to offer fiduciary services, even if the institution does not earn sufficient income to cover the expenses of providing those services.

Ratings to be applied for the alternate rating of earnings. A rating of 1 may be assigned where an institution has implemented all four minimum standards. If fiduciary earnings are lacking, management views this as a cost of doing business as a full-service institution and believes that the negative effects of not offering fiduciary services are more significant than the expense of administrating those services.

A rating of 2 may be assigned where an institution has implemented, at a minimum, three of the four standards. This rating may be assigned if the institution is not generating positive earnings or where formal earnings information may not be available.

A rating of 3 may be assigned if the institution has implemented at least two of the four standards. Although management may have attempted to identify and quantify other revenue to be earned by offering fiduciary services, it has decided that these services should be offered as a service to customers, even if they cannot be operated profitably.

A rating of 4 may be assigned if the institution has implemented only one of the four standards. Management has undertaken little or no effort to identify or quantify the collateral advantages, if any, to the institution from offering fiduciary services.

A rating of 5 may be assigned if the institution has implemented none of the standards.

Compliance

The compliance rating reflects an institution's overall compliance with applicable laws, regulations, accepted standards of fiduciary conduct, governing account instruments, duties associated with account administration, and internally established policies and procedures. This component specifically incorporates an assessment of a fiduciary's duty of undivided loyalty and compliance with applicable laws, regulations, and accepted standards of fiduciary conduct related to self-dealing and other conflicts of interest.

The compliance component includes reviewing and evaluating the adequacy and soundness of adopted policies, procedures, and practices generally and as they relate to specific transactions and accounts. It also includes reviewing policies, procedures, and practices to evaluate the sensitivity of management and the board of directors to refrain from self-dealing, minimize potential conflicts of interest, and resolve actual conflict situations in favor of the fiduciary-account beneficiaries.

Risks associated with account administration are potentially unlimited because each account is a separate contractual relationship that contains specific obligations. Risks associated with account administration include failure to comply with applicable laws, regulations, or terms of the governing instrument; inadequate account-administration practices; and inexperienced man-

agement or inadequately trained staff. Risks associated with a fiduciary's duty of undivided loyalty generally stem from engaging in self-dealing or other conflict-of-interest transactions. An institution may be exposed to compliance, strategic, financial, and reputation risk related to account-administration and conflicts-of-interest activities. The ability of management to identify, measure, monitor, and control these risks is reflected in this rating. Policies, procedures, and practices pertaining to account administration and conflicts of interest are evaluated in light of the size and character of an institution's fiduciary business.

The compliance rating is based on, but not limited to, an assessment of the following evaluation factors:

- compliance with applicable federal and state statutes and regulations, including, but not limited to, federal and state fiduciary laws, the Employee Retirement Income Security Act of 1974, federal and state securities laws, state investment standards, state principal and income acts, and state probate codes
- compliance with the terms of governing instruments
- the adequacy of overall policies, practices, and procedures governing compliance, considering the size, complexity, and risk profile of the institution's fiduciary activities
- the adequacy of policies and procedures addressing account administration
- the adequacy of policies and procedures addressing conflicts of interest, including those designed to prevent the improper use of "material inside information"
- the effectiveness of systems and controls in place to identify actual and potential conflicts of interest
- the adequacy of securities-trading policies and practices relating to the allocation of brokerage business; the payment of services with "soft dollars"; and the combining, crossing, and timing of trades
- the extent and permissibility of transactions with related parties, including, but not limited to, the volume of related commercial and fiduciary relationships and holdings of corporations in which directors, officers, or employees of the institution may be interested
- the decision-making process used to accept, review, and terminate accounts
- the decision-making process related to account-administration duties, including cash balances, overdrafts, and discretionary distributions

Ratings of compliance. A rating of 1 indicates strong compliance policies, procedures, and practices. Policies and procedures covering conflicts of interest and account administration are appropriate in relation to the size and complexity of the institution's fiduciary activities. Accounts are administered in accordance with governing instruments, applicable laws and regulations, sound fiduciary principles, and internal policies and procedures. Any violations are isolated, technical in nature, and easily correctable. All significant risks are consistently and effectively identified, measured, monitored, and controlled.

A rating of 2 indicates fundamentally sound compliance policies, procedures, and practices in relation to the size and complexity of the institution's fiduciary activities. Account administration may be flawed by moderate weaknesses in policies, procedures or practices. Management's practices indicate a determination to minimize the instances of conflicts of interest. Fiduciary activities are conducted in substantial compliance with laws and regulations, and any violations are generally technical in nature. Management corrects violations in a timely manner and without loss to fiduciary accounts. Significant risks are effectively identified, measured, monitored, and controlled.

A rating of 3 indicates compliance practices that are less than satisfactory in relation to the size and complexity of the institution's fiduciary activities. Policies, procedures, and controls have not proven effective and require strengthening. Fiduciary activities may be in substantial noncompliance with laws, regulations, or governing instruments, but losses are no worse than minimal. Although management may have the ability to achieve compliance, the number of violations that exist, or the failure to correct prior violations, is an indication that management has not devoted sufficient time and attention to its compliance responsibilities. Risk-management practices generally need improvement.

A rating of 4 indicates an institution with deficient compliance practices in relation to the size and complexity of its fiduciary activities. Account administration is notably deficient. The institution makes little or no effort to minimize potential conflicts or refrain from self-dealing, and it is confronted with a considerable number of potential or actual conflicts. Numerous substantive and technical violations of laws and

regulations exist, and many may remain uncorrected from previous examinations. Management has not exerted sufficient effort to effect compliance and may lack the ability to effectively administer fiduciary activities. The level of compliance problems is significant and, if left unchecked, may subject the institution to monetary losses or reputation risk. Risks are inadequately identified, measured, monitored, and controlled.

A rating of 5 indicates critically deficient compliance practices. Account administration is critically deficient or incompetent, and there is a flagrant disregard for the terms of the governing instruments and interests of account beneficiaries. The institution frequently engages in transactions that compromise its fundamental duty of undivided loyalty to account beneficiaries. There are flagrant or repeated violations of laws and regulations and significant departures from sound fiduciary principles. Management is unwilling or unable to operate within the scope of laws and regulations or within the terms of governing instruments, and efforts to obtain voluntary compliance have been unsuccessful. The severity of noncompliance presents an imminent monetary threat to account beneficiaries and creates significant legal and financial exposure to the institution. Problems and significant risks are inadequately identified, measured, monitored, or controlled and now threaten the ability of management to continue engaging in fiduciary activities.

Asset Management

The asset-management rating reflects the risks associated with managing the assets (including cash) of others. Prudent portfolio management is based on an assessment of the needs and objectives of each account or portfolio. An evaluation of asset management should consider the adequacy of processes related to the investment of all discretionary accounts and portfolios, including collective investment funds, proprietary mutual funds, and investment advisory arrangements.

The institution's asset-management activities subject it to reputation, compliance, and strategic risks. In addition, each individual account or portfolio managed by the institution is subject to financial risks such as market, credit, liquidity, and interest-rate risk, as well as transaction and compliance risk. The ability of management to identify, measure, monitor, and control these risks is reflected in this rating.

The asset-management rating is based on, but not limited to, an assessment of the following evaluation factors:

- the adequacy of overall policies, practices, and procedures governing asset management, considering the size, complexity, and risk profile of the institution's fiduciary activities
- the decision-making processes used for selection, retention, and preservation of discretionary assets, including adequacy of documentation, committee review and approval, and a system to review and approve exceptions
- the use of quantitative tools to measure the various financial risks in investment accounts and portfolios
- the existence of policies and procedures addressing the use of derivatives or other complex investment products
- the adequacy of procedures related to the purchase or retention of miscellaneous assets, including real estate, notes, closely held companies, limited partnerships, mineral interests, insurance, and other unique assets
- the extent and adequacy of periodic reviews of investment performance, taking into consideration the needs and objectives of each account or portfolio
- the monitoring of changes in the composition of fiduciary assets for trends and related risk exposure
- the quality of investment research used in the decision-making process and documentation of the research
- the due-diligence process for evaluating investment advice received from vendors or brokers (including approved or focus lists of securities)
- the due-diligence process for reviewing and approving brokers or counterparties used by the institution

This rating may not be applicable for some institutions because their operations do not include activities involving the management of any discretionary assets. Functions of this type would include, but not necessarily be limited to, directed-agency relationships, securities clearing, nonfiduciary custody relationships, and transfer-agent and registrar activities. In institutions of this type, the rating for asset management may be omitted by the examiner in accordance with the examining agency's implementing

guidelines. However, this component should be assigned when the institution provides investment advice, even though it does not have discretion over the account assets. An example of this type of activity would be where the institution selects or recommends the menu of mutual funds offered to participant-directed 401(k) plans.

Ratings of asset management. A rating of 1 indicates strong asset-management practices. Identified weaknesses are minor in nature. Risk exposure is modest in relation to management's abilities and the size and complexity of the assets managed.

A rating of 2 indicates satisfactory asset-management practices. Moderate weaknesses are present and are well within management's ability and willingness to correct. Risk exposure is commensurate with management's abilities and the size and complexity of the assets managed. Supervisory response is limited.

A rating of 3 indicates that asset-management practices are less than satisfactory in relation to the size and complexity of the assets managed. Weaknesses may range from moderate to severe; however, they are not of such significance as to generally pose a threat to the interests of account beneficiaries. Asset-management and risk-management practices generally need to be improved. An elevated level of supervision is normally required.

A rating of 4 indicates deficient asset-management practices in relation to the size and complexity of the assets managed. The levels of risk are significant and inadequately controlled. The problems pose a threat to account beneficiaries generally and, if left unchecked, may subject the institution to losses and could undermine the reputation of the institution.

A rating of 5 represents critically deficient asset-management practices and a flagrant disregard of fiduciary duties. These practices jeopardize the interests of account beneficiaries, subject the institution to losses, and may pose a threat to the soundness of the institution.