5000—OTHER EXAMINATION AREAS

The 5000 series of sections provide background on the supervisory assessment of certain bank activities in which a state member bank may or may not engage. These examination activities are sometimes referred to as "specialty examinations" and are conducted by examiners who have subject matter expertise or specialized training. More specifically, there is a section on a bank's fiduciary or asset and wealth management activities. There are also sections that are salient to the supervisory assessment of information technology and payment systems risks.

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 functions 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 (preferably 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,

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.

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 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

4. 12 USC 371c-1(b)(2).

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).

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 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 assessment 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 fidu-

ciary 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 management 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.

Examination procedures are available on the Examination Documentation (ED) modules page on the Board's website. See the following ED module for examination procedures on this topic:

- Trust

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 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, subsidi-

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.

aries, 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."[3] Under the CIP rule, a person that opens a new account is deemed a customer.[4] 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.

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.)

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.

3. 31 CFR 1020.100 (a)(1).

4. 31 CFR 1020.100(c)(1)(i).

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 institution, 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)).[5] 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 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

5. 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.

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. Inde-

pendent 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 viola-

tor 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 world-

wide 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.

Private-Banking Activities
Examination Objectives
Effective date May 2006

Section 5210.2

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).

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 5220.4

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)]

A bank operates as a securities dealer when it underwrites, trades, or deals in securities. These activities may be administered in a separately identifiable trading department or incorporated within the overall treasury department. The organizational structure will generally be a function of the level of activity and the importance of the activity as a product line. If a repetitive pattern of short-term purchases and sales demonstrates that the bank holds itself out to other dealers or investors as a securities dealer, the bank is trading, regardless of what department or section of the bank is engaged in the activity.

The authority under which a bank may engage in securities trading and underwriting is found in section 5136 of the Revised Statutes (12 USC 24 (seventh)). That authority is restricted by limitations on the percentage holding of classes of securities as found in 12 CFR 1.3. This regulation allows banks to deal, underwrite, purchase, and sell (1) type I securities without limit and (2) type II securities subject to a limit of 10 percent of capital and unimpaired surplus per issue. Banks are prohibited from underwriting or dealing in type III securities for their own accounts. See section 2020.1, "Investment Securities and End-User Activities," for further information on types I, II, and III securities.

Banks are involved in three major types of securities transactions. First, the bank, acting as broker, buys and sells securities on behalf of a customer. These are agency transactions in which the agent (bank) assumes no substantial risk and is compensated by a prearranged commission or fee. A second type of securities transaction banks frequently execute is a "riskless-principal" trade. Upon the order of an investor, the dealer buys (or sells) securities through its own account, with the purchase and sale originating almost simultaneously. Because of the brief amount of time the security is held in the dealer's own account, exposure to market risks is limited. Profits result from dealer-initiated markup (the difference between the purchase and sale prices). Finally, as a dealer, the bank buys and sells securities for its own account. This is termed a principal transaction because the bank is acting as a principal, buying or selling qualified securities through its own inventory and absorbing whatever market gain or loss is made on the transaction.

The volume of bank dealer activity and the dealer's capacity in the transaction are critical to an examiner's assessment regarding the examination scope and the required examiner resources and expertise. Dealers engaging primarily in agency or riskless-principal transactions are merely accommodating customers' investment needs. Market risk will be nominal, and the key examination concern will be operational risk and efficiency. Active dealers generally carry larger inventory positions and may engage in some degree of proprietary trading. Their market-risk profile may be moderate to high.

Bank dealers' securities transactions involve customers and other securities dealers. The word "customer," as used in this section, means an investor. Correspondent banks purchasing securities for an investment account would also be considered a customer. Transactions with other dealers are not considered customer transactions unless the dealer is buying or selling for investment purposes.

The following subsections include general descriptions of significant areas of bank trading and underwriting activities. Foreign exchange is covered in detail in the "International" sections of this manual. Additional bank dealer activities, particularly in derivative products, are extensively covered in the *Trading and Capital-Markets Activities Manual*. In addition, many money-center banks and larger regional banks have transferred dealing activities to separately capitalized holding company subsidiaries (known as underwriting affiliates). The *Bank Holding Company Supervision Manual* contains a separate section on nonbank subsidiaries engaged in underwriting and dealing in bank-ineligible securities.

OVERVIEW OF RISK

For bank dealer activities, risk is generally defined as the potential for loss on an instrument or portfolio. Significant risk can also arise from operational weakness and inadequate controls. Risk management is the process by which managers identify, assess, and control all risks associated with a financial institution's activities. The increasing complexity of the financial industry and the range of financial instruments banks use have made risk management more difficult

to accomplish and evaluate.

The four fundamental elements for evaluating the risk-management process for bank dealer activities are—

- active board and management oversight,
- adequate risk-management policies and limits,
- appropriate risk measurement and management information systems, and
- comprehensive internal controls and audit procedures.

For risk management to be effective, an institution's board and senior management must be active participants in the process. They must ensure that adequate policies and risk-tolerance limits are developed for managing the risk in bank dealer activities, and they must understand, review, and approve these limits across all established product lines. For policies and limits to be effective and meaningful, risk measures, reports, and management information systems must provide management and the board with the information and analysis necessary to make timely and appropriate responses to changing conditions. Risk management must also be supported by comprehensive internal controls and audit procedures that provide appropriate checks and balances to maintain an ongoing process of identifying any emerging weaknesses in an institution's management of risk.[1] At a minimum, the effectiveness of the institution's policies, limits, reporting systems, and internal controls must be reviewed annually.

In assessing the adequacy of the above elements at individual institutions, examiners should consider the nature and volume of a bank's dealer activities and its overall approach toward managing the various types of risks involved. The sophistication or complexity of policies and procedures used to manage risk depends on the bank dealer's chosen products, activities, and lines of business. Accordingly, examiners should expect risk-management activities to differ among institutions.

As a financial institution's product offerings and geographic scope expand, examiners must review the risk-management process not only by business line, but on a global, consolidated basis. In more sophisticated institutions, the role of risk management is to identify the risks associated with particular business activities and to aggregate summary data into generic components, ultimately allowing exposures to be evaluated on a common basis. This methodology enables institutions to manage risks by portfolio and to consider exposures in relationship to the institution's global strategy and risk tolerance.

A review of the global organization may reveal risk concentrations that are not readily identifiable from a limited, stand-alone evaluation of a branch, agency, Edge Act institution, nonbank subsidiary, or head office. Consolidated risk management also allows the institution to identify, measure, and control its risks, while giving necessary consideration to the breakdown of exposure by legal entity. Sometimes, if applicable rules and laws allow, identified risks at a branch or subsidiary may be offset by exposures at another related institution. However, risk management across separate entities must be done in a way that is consistent with the authorities granted to each entity. Some financial institutions and their subsidiaries may not be permitted to hold, trade, deal, or underwrite certain types of financial instruments unless they have received special regulatory approval. Examiners should ensure that a financial institution only engages in those activities for which it has received regulatory approval. Furthermore, examiners should verify that the activities are conducted in accordance with any Board conditions or commitments attached to the regulatory approval.

Ideally, an institution should be able to identify its relevant generic risks and should have measurement systems in place to quantify and control these risks. While it is recognized that not all institutions have an integrated risk-management system that aggregates all business activities, the ideal management tool would incorporate a common measurement denominator. Risk-management methodologies in the marketplace and an institution's scope of business are continually evolving, making risk management a dynamic process. Nonetheless, an institution's risk-management system should always be able to identify, aggregate, and control all risks posed by underwriting, trading, or dealing in securities that could have a significant impact on capital or equity.

Trading and market-risk limits should be customized to address the nature of the products

1. Existing policies and examiner guidance on various topics applicable to the evaluation of risk-management systems can be found in SR-93-69, "Examining Risk Management and Internal Controls for Trading Activities of Banking Organizations." Many of the managerial and examiner practices contained in this document are fundamental and are generally accepted as sound practices for trading activities.

and any unique risk characteristics. Common types of limits include earnings-at-risk limits, stop-loss limits, limits on notional amounts (both gross and duration-weighted), maturity limits, and maturity-gap limits. The level of sophistication needed within the limit matrix will depend on the type of instrument involved and the relative level of trading activity. Straightforward notional and tenor limits may be adequate for most dealers; however, dealers involved in a wide array of products and more complex transactions will need stronger tools to measure and aggregate risk across products.

In general, risk from trading and dealing activities can be broken down into the following categories:

- Market or price risk is the exposure of an institution's financial condition to adverse movements in the market rates or prices of its holdings before such holdings can be liquidated or expeditiously offset. It is measured by assessing the effect of changing rates or prices on either the earnings or economic value of an individual instrument, a portfolio, or the entire institution.
- Funding-liquidity risk refers to the ability to meet investment and funding requirements arising from cash-flow mismatches.
- Market-liquidity risk refers to the risk of being unable to close out open positions quickly enough and in sufficient quantities at a reasonable price.
- Credit risk is the risk that a counterparty to a transaction will fail to perform according to the terms and conditions of the contract, thus causing the security to suffer a loss in cash-flow or market value. Because securities settlements are typically "delivery vs. payment" and settlement periods are relatively short, securities transactions do not involve a significant level of counterparty credit risk. Repurchase transactions, securities lending, and money market transactions, however, involve significantly higher levels of credit risk if not properly controlled. As a result, credit risk is discussed in greater detail in the subsections addressing these products. Credit risk can also arise from positions held in trading inventory. Although U.S. government and agency securities do not generally involve credit risk, other securities (for example, municipal and corporate securities) carried in inventory can decline in price due to a deterioration in credit quality.
- Clearing or settlement risk is (1) the risk that a counterparty who has received a payment or delivery of assets defaults before delivery of the asset or payment or (2) the risk that technical difficulties interrupt delivery or settlement despite the counterparty's ability or willingness to perform.
- Operations and systems risk is the risk of human error or fraud, or the risk that systems will fail to adequately record, monitor, and account for transactions or positions.
- Legal risk is the risk that a transaction cannot be consummated as a result of some legal barrier, such as inadequate documentation, a regulatory prohibition on a specific counterparty, non-enforceability of bilateral and multilateral close-out netting, or collateral arrangements in bankruptcy.

The *Trading and Capital-Markets Activities Manual* contains a comprehensive discussion of these risks, including examination objectives, procedures, and internal control questionnaires by risk category.

GOVERNMENT AND AGENCY SECURITIES

The government securities market is dominated by a number of investment banks, broker-dealers, and commercial banks known as primary dealers in government securities. These dealers make an over-the-counter market in most government and federal-agency securities. Primary dealers are authorized to deal directly with the Open Market Desk of the Federal Reserve Bank of New York. As market makers, primary dealers quote bid-ask prices on a wide range of instruments, and many publish daily quotation sheets or provide live electronic data feeds to larger customers or other dealers.

Government securities trading inventories are generally held with the objective of making short-term gains through market appreciation and dealer-initiated markups. Common factors that affect the markup differential include the size of a transaction, the dealer efforts extended, the type of customer (active or inactive), and the nature of the security. Markups on government securities generally range between 1/32 and 4/32 of a point. Long-maturity issues or derivative products may have higher markups due to the higher

risk and potentially larger volatility that may be inherent in these products.

According to industry standards, payments for and deliveries of U.S. government and most agency securities are settled one business day following the trade date, although government dealers and customers can negotiate same-day or delayed settlement for special situations.

When-Issued Trading

A significant potential source of risk to dealers involves "when-issued" (WI) trading in government securities. WI trading is the buying and selling of securities in the one- to two-week interim between the announcement of an offering and the security auction and settlement. Although the vast majority of transactions settle on the next business day, WI trading results in a prolonged settlement period. This could increase both the market risk and counterparty credit risk associated with trading these instruments. The prolonged settlement period also provides an opportunity for a dealer to engage in a large volume of off-balance-sheet trading without having to fund the assets or cover the short positions. In essence, WI trading allows the dealers to create securities. If the overall level of WI trading is significant in relation to the size of the issue, the resulting squeeze on the market could increase volatility and risk. Given these potential risk characteristics, WI trading should be subject to separate sublimits to cap the potential exposure.

Short Sales

Another area of U.S. government securities activity involves short-sale transactions. A short sale is the sale of a security that the seller does not own at the time of the sale. Delivery may be accomplished by buying the security or by borrowing the security. When the security delivered is borrowed, the short seller likely will ultimately have to acquire the security in order to satisfy its repayment obligation. The borrowing transaction is collateralized by a security (or securities) of similar value or cash (most likely the proceeds of the short sale). Reverse repurchase transactions are also used to obtain the security needed to make delivery on the security sold short. Carrying charges on borrowed government securities should be deducted from the short sale and purchase spread to determine net profit. Short sales are conducted to (1) accommodate customer orders, (2) obtain funds by leveraging existing assets, (3) hedge the market risk of other assets, or (4) allow a dealer to profit from a possible future decline in market price by purchasing an equivalent security at a later date at a lower price.

Government Securities Clearing

Securities-clearing services for the bulk of U.S. government securities transactions and many federal-agency securities transactions are provided by the Federal Reserve as part of its electronic securities-transfer system. The various Federal Reserve Banks will wire-transfer most government securities between the book-entry safekeeping accounts of the seller and buyer. The Federal Reserve's systems are also used to facilitate security borrowings, loans, and pledges.

Government Securities Act

In response to the failures of a number of unregulated government securities dealers between 1975 and 1985, Congress passed the Government Securities Act of 1986 (GSA). GSA established, for the first time, a federal system for the regulation of the entire government securities market, including previously unregulated brokers and dealers. The primary goal of GSA was to protect investors and ensure the maintenance of a fair, honest, and liquid market.

The GSA granted the Department of the Treasury (Treasury) authority to develop and implement rules for transactions in government and agency securities effected by government securities brokers or dealers (that is, securities firms as well as other financial institutions), and to develop and implement regulations relating to the custody of government securities held by depository institutions. The rules were intended to prevent fraudulent and manipulative acts and practices and to protect the integrity, liquidity, and efficiency of the government securities market. At the same time, the rules were designed to preclude unfair discrimination among brokers, dealers, and customers. Enforcement of the rules

for the GSA is generally carried out by an institution's primary regulatory organization.

The rules for the GSA had the most significant effect on those entities that were not previously subject to any form of federal registration and regulation. These entities included not only firms registered as government securities brokers or dealers but also firms registered as brokers or dealers trading in other securities and financial products. For the first time, the government securities activities of these entities were subject to the discipline of financial responsibility, customer protection, recordkeeping, and advertising requirements. For nonbank dealers, this regulation is enforced by a self-regulatory organization, the Financial Industry Regulatory Authority (FINRA), which conducts routine examinations under the oversight of the Securities and Exchange Commission (SEC).

The provisions of the GSA that had the most significant effect on government securities brokers and dealers (both bank and nonbank broker-dealers) relate to hold-in-custody repurchase agreement rules. Congress targeted this area because of abuses that had resulted in customer losses. Several requirements to strengthen customer protection were imposed: (1) written repurchase agreements must be in place, (2) the risks of the transactions must be disclosed to the customer, (3) specific repurchase securities must be allocated to and segregated for the customer, and (4) confirmations must be made and provided to the customer by the end of the day on which a transaction is initiated and on any day on which a substitution of securities occurs. For a more detailed description of the rules for the GSA requirements, see the procedures for the examination of government securities activities issued by the Board of Governors of the Federal Reserve System, or 17 CFR 400–450 for the actual text of the regulations.

Registration Exemptions

Most banks acting as government securities brokers or dealers are required to file a form known as a G-FIN. This form details the bank's capacity, the locations where government securities activities are performed, and the persons responsible for supervision. However, certain bank government securities activities are exempt from the filing requirements. Banks handling only U.S. savings bond transactions or submitting tender offers on original issue U.S. Treasury securities are exempt from registration.

Limited government securities brokerage activities are also exempt from registration under certain circumstances. Banks that engage in fewer than 500 government securities transactions annually (excluding savings bond transactions and Treasury tender offers) are exempt. Similarly, banks are exempt if they deal with a registered broker-dealer under a ''networking'' arrangement, assuming they meet the following conditions: (1) the transacting broker must be clearly identified, (2) bank employees perform only clerical or administrative duties and do not receive transaction-based compensation, and (3) the registered broker-dealer receives and maintains all required information on each customer. Exempt networking arrangements must be fully disclosed to the customer. Finally, banks are exempt from registration requirements if their activities are limited to purchases and sales in a fiduciary capacity or purchases and sales of repurchase or reverse repurchase agreements.

The preceding exemptions provide relief from registration, but exempt banks must comply (if applicable) with regulations addressing custodial holdings for customers (17 CFR 450). Additionally, banks effecting repurchase/reverse repurchase agreements must comply with repurchase-transaction requirements detailed in 17 CFR 403.5(d).

MUNICIPAL SECURITIES

Municipal securities are debt obligations issued by state and local governments and certain agencies and authorities. There are two broad categories of municipal bonds: general obligation bonds and revenue bonds. General obligation bonds (GOs) are backed by the full faith and credit and taxing authority of the government issuer. General obligation bonds are either limited or unlimited tax bonds. Limited tax bonds are issued by government entities whose taxing authority is limited to some extent by law or statute. For instance, a local government may face restrictions on the level of property taxes it can levy on property owners. State and local entities may also issue special tax bonds, which are supported by a specific tax. For instance, a highway project may be financed by a special

gasoline tax levied to pay for the bonds. Unlimited tax bonds are issued by government entities that are not restricted by law or statute in the amount of taxes they can levy; however, there may be some political limitations.

Municipal revenue bonds are backed by a specific project or government authority, and they are serviced by fees and revenues paid by users of the government entity. Revenue bonds are backed by public power authorities, nonprofit hospitals, housing authorities, transportation authorities, and other public and quasi-public entities.

Effective March 13, 2000, well-capitalized state member banks were authorized by the Gramm-Leach-Bliley Act (GLB Act) to deal in, underwrite, purchase, and sell municipal revenue bonds without any limitations based on the bank's capital. (See 12 USC 24 (seventh).) Previously, banks were limited to only underwriting, dealing in, or investing in, without limitation, general obligation municipal bonds backed by the full faith and credit of an issuer with general powers of taxation. Member banks could invest in, but not underwrite or deal in, municipal revenue bonds, but the purchases and sales of such investment securities for any obligor were limited to 10 percent of a member bank's capital and surplus. As a result of the GLB Act amendment, municipal revenue bonds are the equivalent of type I securities for well-capitalized state member banks.[2] (See SR-01-13.) Banks that are not well capitalized may engage in more limited municipal securities activities relating to type II and type III securities. For example, banks may also deal in, underwrite, or invest in revenue bonds that are backed by housing, university, or dormitory projects.

In addition to municipal bonds, state and local governments issue obligations to meet short-term funding needs. These obligations are normally issued in anticipation of some specific revenue. The types of debt issued include tax-anticipation notes (TANs), revenue-anticipation notes (TRANs), grants-anticipation notes (GANs), bond-anticipation notes (BANs), commercial paper, and others.

Because of the large number and diverse funding needs of state and local governments (over 50,000 state and local governments have issued debt in the United States), there is a wide variety of municipal securities. Some municipal security issues have complex structures that require an increased level of technical expertise to evaluate. As with all areas of banking, dealers who invest in complex instruments are expected to understand the characteristics of the instruments and how these instruments might affect their overall risk profile. While there are some large issuers, like the states of New York and California, most issuers are small government entities that place modest amounts of debt. Many of these issues are exempt from federal, state, and local income taxes; these exemptions, in part, determine the investor base for municipal bonds.

The customer base for tax-exempt municipal securities is investors who benefit from income that is exempt from federal income tax. This group includes institutional investors, such as insurance companies, mutual funds, and retail investors, especially individuals in high income-tax brackets.

Credit Risk

Municipal securities activities involve differing degrees of credit risk depending on the financial capacity of the issuer. Larger issuers of municipal securities are rated by nationally recognized rating agencies (Moody's, S&P, etc.). Other municipalities achieve an investment-grade rating through the use of credit enhancements, usually in the form of a standby letter of credit issued by a financial institution. Banks are also involved in underwriting and placing nonrated municipal securities. Nonrated issues are typically small and are placed with a limited number of investors. Liquidity in the secondary market is limited, and bank dealers rarely carry nonrated issues in trading inventory.

Management should take steps to limit undue concentrations of credit risk arising from municipal-security underwriting and dealing. Exposure to nonrated issuers should be approved through the bank's credit-approval process with appropriate documentation to support the issuer's financial capacity. Activity in nonrated issues outside the bank's target or geographic market should also be avoided. In addition, exposure should be aggregated on a consolidated basis, taking into account additional credit

2. The Office of the Comptroller of the Currency published final amendments to its investment securities regulation (12 CFR 1) on July 2, 2001. (See 66 *Fed. Reg.* 34784.)

risk arising from traditional banking products (loans, letters of credit, etc.).

Municipal Securities Rulemaking Board

The Securities Act Amendments of 1975 (15 USC 78o-4) extended a comprehensive network of federal regulation to the municipal securities markets. Pursuant to the act, municipal securities brokers and dealers are required to register with the SEC. The act also created a separate, self-regulatory body, the Municipal Securities Rulemaking Board (MSRB), to formulate working rules for the regulation of the municipal securities industry. The Federal Reserve is required to ensure compliance with those rules as they apply to state member banks.

A bank engaged in the business of buying and selling municipal securities must register with the SEC as a municipal securities dealer if it is involved in—

- underwriting or participating in a syndicate or joint account for the purpose of purchasing securities;
- maintaining a trading account or carrying dealer inventory; or
- advertising or listing itself as a dealer in trade publications, or otherwise holding itself out to other dealers or investors as a dealer.

Generally, a bank that buys and sells municipal securities for its investment portfolio or in a fiduciary capacity is not considered a dealer.

If a bank meets the SEC's criteria for registering as a municipal securities dealer, it must maintain a separately identifiable department or division involved in municipal securities dealing that is under the supervision of officers designated by the bank's board of directors. These designated officers are responsible for municipal securities dealer activities and should maintain separate records.

The Federal Reserve conducts a separate examination of the municipal securities dealer activities in banks that engage in such activities. This examination is designed to ensure compliance with the rules and standards formulated by the MSRB. For a complete description of the activities of a municipal securities dealer and detailed procedures performed by the Federal Reserve examiners, see the *Municipal Securities Dealer Bank Examination Manual* issued by the Board of Governors of the Federal Reserve System.

REPURCHASE AGREEMENTS AND SECURITIES LENDING

Repurchase agreements (repos) play an important role in the securities markets. A repo is the simultaneous agreement to sell a security and repurchase it at a later date. Reverse repos are the opposite side of the transaction, securities purchased with a later agreement to resell. From the dealer's perspective, a repo is a financing transaction (liability), and a reverse repo is a lending transaction (asset). Overnight repos are a one-day transaction; anything else is referred to as a "term repo." Approximately 80 percent of the repo market is overnight. Although any security can be used in a repurchase transaction, the overwhelming majority of transactions involve government securities.

Securities dealers use repos as an important source of liquidity. The majority of government securities trading inventory will typically be financed with repos. Reverse repos are used to obtain securities to meet delivery obligations arising from short positions or from the failure to receive the security from another dealer. Reverse repos also are an effective and low-risk means to invest excess cash on a short-term basis.

The repo rate is a money market rate that is lower than the federal funds rate due to the collateralized nature of the transaction. Opportunities also arise to obtain below-market-rate financing. This situation arises when demand exceeds supply for a specific bond issue and it goes on "special." Dealers who own the bond or control it under a reverse repo transaction can earn a premium by lending the security. This premium comes in the form of a below-market-rate financing cost on a repo transaction.

Many of the larger dealers also engage in proprietary trading of a matched book, which consists of a moderate to large volume of offsetting repos and reverse repos. The term "matched book" is misleading as the book is rarely perfectly matched. Although profit may be derived from the capture of a bid/ask spread on matched transactions, profit is more often derived from maturity mismatches. In a falling-rate environment, traders lend long (reverse

repos) and borrow short (repos). It is more difficult to profit in rising-rate environments because of the shape of the yield curve, which is usually upward-sloping. The overall size of the matched book and the length of the maturity mismatches will generally decline in a rising environment. Matched books are also used to create opportunities to control securities that may go on special, resulting in potential profit opportunities. Dealers engaging in matched-book trading provide important liquidity to the repo market.

Risk in a matched book should be minimized by establishing prudent limits on the overall size of the book, size of maturity mismatches, and restrictions on the maximum tenor of instruments. The overall risk of a matched book is usually small in relation to other trading portfolios. Maturity mismatches are generally short-term, usually 30 to 60 days, but may extend up to one year. Risk can be quickly neutralized by extending the maturity of assets or liabilities. Financial instruments (futures and forward rate agreements) can also be used to reduce risk.

Securities dealers may also engage in "dollar-roll" transactions involving mortgage-backed securities, which are treated as secured financings for accounting purposes. The "seller" of the security agrees to repurchase a "substantially identical" security from the "buyer," rather than the same security. Many of the supervisory considerations noted above for repurchase agreements also apply to dollar-roll transactions. However, if the security to be repurchased is not substantially identical to the security sold, the transaction generally should be accounted for as a sale and not as a financing arrangement. The accounting guidance for "substantially identical" is described in American Institute of Certified Public Accountants (AICPA) Statement of Position 90-3, which generally requires debt instruments to have the same primary obligor or guarantor, the same form and type, the identical contractual interest rate, the same maturity or weighted average maturity, and other factors.

In addition, securities dealers may engage in securities lending or borrowing transactions. In substance, these transactions are very similar to repo transactions except the transactions have no stated maturity. The transactions are conducted through open-ended "loan" agreements that may be terminated on short notice by the lender or borrower. Although lending transactions have historically been centered in corporate debt and equity obligations, the market increasingly involves loans of large blocks of U.S. government and federal-agency securities. To participate in this market, a bank may lend securities held in its investment account or trading account. Like repos, securities are lent to cover fails (securities sold but not available for delivery) and short sales. Collateral for the transactions can consist of other marketable securities or standby letters of credit; however, the large majority of transactions are secured by cash. Investors are willing to lend securities due to the additional investment income that can be earned by investing the cash collateral. When a securities loan is terminated, the securities are returned to the lender and the collateral to the borrower.

Credit Risk

Since repurchase agreements and securities lending transactions are collateralized, credit risk is relatively minor if properly controlled. Some dealers have underestimated the credit risk associated with the performance of the counterparty and have not taken adequate steps to ensure their control of the securities serving as collateral. The market volatility of the securities held as collateral can also add to the potential credit risk associated with the transaction.

As an added measure of protection, dealers require customers to provide excess collateral. This excess is referred to as "margin." The size of the margin will be a function of the volatility of the instrument serving as collateral and the length of the transaction. In addition to initial margin, term repos and security lending arrangements require additional margin if the value of the collateral declines below a specified level. Excess margin is usually returned to the counterparty if the value of the collateral increases. A daily "mark-to-market" or valuation procedure must be in place to ensure that calls for additional collateral are made on a timely basis. The valuation procedures should be independent of the trader and take into account the value of accrued interest on debt securities. It is important to point out that credit risk can arise from both asset transactions (reverse repos and securities borrowed) and liability transactions (repos and securities lent) because of market fluctuations in collateral provided and received. Deal-

ers should take steps to ensure that collateral provided is not excessive.

Policies and procedures should be in place to ensure transactions are conducted only with approved counterparties. Credit-limit approvals should be based on a credit analysis of the borrower. An initial review should be performed before establishing a relationship, with periodic reviews thereafter. Credit reviews should include an analysis of the bor-rower's financial statement, capital, management, earnings, business reputation, and any other relevant factors. Analyses should be performed in an independent department of the lender institution, by persons who routinely perform credit analyses. Analyses performed solely by the person managing the repo or securities lending programs are not sufficient. Credit and concentration limits should take into account other extensions of credit by other departments of the bank or affiliates. Procedures should be established to ensure that credit and concentration limits are not exceeded without proper authorization from management.

Other Uses and Implications of Securities Lending

In addition to lending their own securities, financial institutions have become increasingly involved in lending customers' securities held in custody, safekeeping, trust, or pension accounts. These activities are typically organized within the bank's trust department. Not all institutions that lend securities or plan to do so have relevant experience. Because the securities available for lending often greatly exceed the demand, inexperienced lenders may be tempted to ignore commonly recognized safeguards. Bankruptcies of broker-dealers have heightened regulatory sensitivity to the potential for problems in this area.

Fees received on securities loans are divided between the custodial institution and the customer account that owns the securities. In situations involving cash collateral, part of the interest earned on the temporary investment of cash is returned to the borrower and the remainder is divided between the lender institution and the customer account that owns the securities.

In addition to a review of controls, examiners should take steps to ensure that cash collateral is invested in appropriate instruments. Cash should be invested in high-quality, short-term money market instruments. Longer-term floating-rate instruments may also be appropriate; however, illiquid investments and products with customized features (for example, structured notes with imbedded options) should be avoided. Several banks have reported significant losses associated with inappropriate investments in securities lending areas.

Securities-Lending Capacity

Securities lending may be done in various capacities and with differing associated liabilities. It is important that all parties involved understand in what capacity the lender institution is acting. The relevant capacities are described below.

Principal

A lender institution offering securities from its own account is acting as principal. A lender institution offering customers' securities on an undisclosed basis is also considered to be acting as principal.

Agent

A lender institution offering securities on behalf of a customer-owner is acting as an agent. To be considered a bona fide or ''fully disclosed'' agent, the lending institution must disclose the names of the borrowers to the customer-owners and the names of the customer-owners to the borrowers (or give notice that names are available upon request). In all cases, the agent's compensation for handling the transaction should be disclosed to the customer-owner. Undisclosed agency transactions, that is, ''blind brokerage'' transactions in which participants cannot determine the identity of the contra party, are treated as if the lender institution were the principal.

Directed Agent

A lender institution that lends securities at the direction of the customer-owner is acting as a

directed agent. The customer directs the lender institution in all aspects of the transaction, including to whom the securities are loaned, the terms of the transaction (rebate rate and maturity/call provisions on the loan), acceptable collateral, investment of any cash collateral, and collateral delivery.

Fiduciary

A lender institution that exercises discretion in offering securities on behalf of and for the benefit of customer-owners is acting as a fiduciary. For supervisory purposes, the underlying relationship may be as agent, trustee, or custodian.

Finder

A finder brings together a borrower and a lender of securities for a fee. Finders do not take possession of the securities or collateral. Delivery of securities and collateral is directly between the borrower and the lender, and the finder does not become involved. The finder is simply a fully disclosed intermediary.

MONEY MARKET INSTRUMENTS

In addition to bank-eligible securities activities, banks may engage in a substantial volume of trading in money market instruments. Federal funds, banker's acceptances, commercial paper, and certificates of deposit are forms of money market instruments. While these instruments may be used as part of the overall funding strategy, many firms actively engage in discretionary or proprietary trading in these instruments. As in matched-book repo activities, profits from trading money market instruments are derived from the bid/ask spread on matched transactions and the net interest spread from maturity mismatches.

This activity may result in overall money market arbitrage. Arbitrage is the coordinated purchase and sale of the same security or its equivalent, for which there is a relative price imbalance in the market. The objective of such activity is to obtain earnings by taking advantage of changing yield spreads. Arbitrage can occur with items such as Eurodollar CDs, banker's acceptances, and federal funds, and with financial instruments such as futures and forwards.

Although the risk of money market trading is relatively straightforward, the potential risk can be significant based on the volume of trading and size of the mismatches. Despite the potential risk, these activities may offer attractive profit opportunities if effectively controlled. Short-term interest-rate markets are very liquid, and risk can be quickly neutralized by changing the maturity profile of either assets or liabilities. Financial instruments (such as futures and forward rate agreements) can also be an effective tool to manage risk. Money market trading may be managed as a separate product line or may be integrated with trading in other interest-rate products (such as swaps, caps, or floors). Examiners should take steps to ensure that appropriate limits are in place for money market trading, including restrictions on aggregate notional size, the size of maturity mismatches, and the maximum tenor of instruments.

Federal Funds

Commercial banks actively use the federal funds market as a mechanism to manage fluctuations in the size and composition of their balance sheet. Federal funds are also an efficient means to manage reserve positions and invest excess cash on a short-term basis. Although transactions are generally unsecured, they can also be secured. The majority of transactions are conducted overnight; however, term transactions are also common. Federal funds trading will often involve term transactions in an attempt to generate positive net interest spread by varying the maturities of assets and liabilities.

Banks have traditionally engaged in federal funds transactions as principal, but an increasing number of banks are conducting business as agent. These agency-based federal funds transactions are not reported on the agent's balance sheet. Dealer banks may also provide federal funds clearing services to their correspondent banks.

Banker's Acceptances

Banker's acceptances are time drafts drawn on and accepted by a bank. They are the customary

means of effecting payment for merchandise sold in import-export transactions, as well as a source of financing used extensively in international trade. Banker's acceptances are an obligation of the acceptor bank and an indirect obligation of the drawer. They are normally secured by rights to the goods being financed and are available in a wide variety of principal amounts. Maturities are generally less than nine months. Acceptances are priced like Treasury bills, with a discount figured for the actual number of days to maturity based on a 360-day year. The bank can market acceptances to the general public but must guarantee their performance.

Commercial Paper

Commercial paper is a generic term that is used to describe short-term, unsecured promissory notes issued by well-recognized and generally sound corporations. The largest issuers of commercial paper are corporations, bank holding companies, and finance companies, which use the borrowings as a low-cost alternative to bank financing. Commercial paper is exempt from registration under the Securities Act of 1933 if it meets the following conditions:

- prime quality and negotiable
- not ordinarily purchased by the general public
- issued to facilitate current operational business requirements
- eligible for discounting by a Federal Reserve Bank
- maturity does not exceed nine months

Actively traded commercial paper is ordinarily issued in denominations of at least $100,000 and often in excess of $1 million. Commercial paper issuers usually maintain unused bank credit lines to serve as a source of back-up liquidity or contingency financing, principally in the form of standby letters of credit. Major commercial paper issuers are rated by nationally recognized rating agencies (Moody's, S&P, and others). Other issuers achieve higher ratings through the use of a credit enhancement, usually in the form of a standby letter of credit issued by a financial institution.

Based on Supreme Court rulings, commercial paper was considered a security for purposes of the former Glass-Steagall Act. As a result, banks were generally prohibited from underwriting and dealing in commercial paper. Despite this restriction, banks participated in this market in an "agency capacity." When establishing a commercial paper dealership, many of the larger banks pursued business through an aggressive interpretation of an agency-transaction role. In practice, bank dealers engage in riskless-principal or best-efforts placement of commercial paper. Taking this logic a step further, others actively engage in competitive bidding and intraday distribution of newly issued paper. Because the paper settles on a same-day basis, the transactions are never part of the official end-of-day records of the bank. Although this technical point has been the subject of discussion, the practice has not been subject to regulatory challenge.

Commercial paper may be issued as an interest-bearing instrument or at a discount. Market trades are priced at a current yield, net of accrued interest due the seller or, if the commercial paper was issued at a discount, at a discount figured for the actual number of days to maturity based on a 360-day year.

The sale of commercial paper issued by bank affiliates must conform to legal restrictions and avoid conflicts of interest. Each certificate and confirmation should disclose the facts that the commercial paper is not a deposit and is not insured by the Federal Deposit Insurance Corporation.

Certificates of Deposit

Negotiable certificates of deposit (CDs) issued by money-center banks are actively traded in denominations of $100,000 to $1 million. Interest generally is calculated on a 360-day year and paid at maturity. Secondary-market prices are computed based on current yield, net of accrued interest due the seller. Eurodollar CDs trade like domestic CDs except their yields are usually higher and their maturities are often longer.

Credit-Risk and Funding Concentrations

In addition to market risk, money market policies and guidelines should recognize the credit risk inherent in these products. Federal funds sold and deposit placements are essentially un-

secured advances. To avoid undue concentrations of credit risk, activity with these products should be limited to approved counterparties. Limits should be established for each prospective counterparty. Tenor limits should also be considered to reduce the potential for credit deterioration over the life of the transaction. The size of limits should be based on both anticipated activity and the counterparty's financial capacity to perform. The credit analysis should be performed by qualified individuals in a credit department that is independent from the money market dealing function. In assessing the creditworthiness of other organizations, institutions should not rely solely on outside sources, such as standardized ratings provided by independent rating agencies, but should perform their own analysis of a counterparty's or issuer's financial strength. At a minimum, limits should be reassessed and credit analyses updated annually. Once established, limits should be monitored with exceptions documented and approved by the appropriate level of senior management. Exposure should also be aggregated on a consolidated basis with any other credit exposure arising from other product areas. Exposure to foreign bank counterparties should also be aggregated by country of domicile to avoid country-risk concentrations. The limit structure should be reviewed to ensure compliance with the requirements of Regulation F, Limitations on Interbank Liabilities, which places prudent limits on credit exposure to correspondent banks.

Maintaining a presence in the wholesale funding markets requires a strong reputation and increases potential liquidity risk. The prolonged use of a large volume of purchased funds to support a money market trading operation could also reduce the capacity to tap this market, if needed, for core funding. Guidelines should be in place to diversify sources of funding. Contingency plans should include strategies to exit or reduce the profile in these markets if the situation warrants.

OPERATIONS AND INTERNAL CONTROLS

A bank dealer's operational functions should be designed to regulate the custody and movement of securities and to adequately account for trading transactions. Because of the dollar volume and speed of trading activities, operational inefficiencies can quickly result in major problems.

Sound Practices for Front- and Back-Office Operations

Bank dealer activities vary significantly among financial institutions, depending on the size and complexity of the trading products; trading, back-office, and management expertise; and the sophistication of systems. As a result, practices, policies, and procedures in place in one institution may not be necessary in another. The adequacy of internal controls requires sound judgment on the part of the examiner. The following is a list of policies and procedures that should be reviewed:

- Every organization should have comprehensive policies and procedures in place that describe the full range of bank dealer activities performed. These documents, typically organized into manuals, should at a minimum address front- and back-office operations; reconciliation guidelines and frequency; revaluation and accounting guidelines; descriptions of accounts; broker policies; a code of ethics; and the risk-measurement and -management methods, including a comprehensive limit structure.
- Every institution should have existing policies and procedures to ensure the segregation of duties among the trading, control, and payment functions.
- Revaluation sources should be independent from the traders for accounting purposes, risk oversight, and senior management reporting, although revaluation of positions may be conducted by traders to monitor positions.
- Trader and dealer telephone conversations should be taped to facilitate the resolution of disputes and to serve as a valuable source of information to auditors, managers, and examiners.
- Trade tickets and blotters (or their electronic equivalents) should be timely and complete to allow for easy reconciliation and for appropriate position and exposure monitoring. The volume and pace of trading may warrant virtually simultaneous creation of these records in some cases.
- Computer hardware and software applications must have the capacity to accommodate the

current and projected level of trading activity. Appropriate disaster-recovery plans should be tested regularly.
- Every institution should have a methodology to identify and justify any off-market transactions. Ideally, off-market transactions would be forbidden.
- A clear institutional policy should exist for personal trading. If such trading is permitted at all, procedures should be established to avoid even the appearance of conflicts of interest.
- Every institution should ensure that the management of after-hours and off-premises trading, if permitted at all, is well documented so that transactions are not omitted from the automated blotter or the bank's records.
- Every institution should ensure that staff is both aware of and complies with internal policies governing the trader-broker relationship.
- Every institution that uses brokers should monitor the patterns of broker usage, be alert to possible undue concentrations of business, and review the list of approved brokers at least annually.
- Every institution that uses brokers should establish a policy that minimizes name substitutions of brokered transactions. All such transactions should be clearly designated as switches, and relevant credit authorities should be involved.
- Every institution that uses brokers for foreign-exchange transactions should establish a clear statement forbidding the lending or borrowing of brokers' points as a method to resolve discrepancies.
- Every organization should have explicit compensation policies to resolve disputed trades for all traded products. Under no circumstances should "soft-dollar" (the exchange of services in lieu of dollar compensation) or off-the-books compensation be permitted for dispute resolution.
- Every institution should have know-your-customer policies, and they should be understood and acknowledged by trading and sales staff.
- The designated compliance officer should perform a review of trading practices at least annually. In institutions with a high level of trading activity, interim reviews may be warranted.
- The organization should have an efficient confirmation-matching process that is fully independent from the dealing function. Documentation should be completed and exchanged as close to completion of a transaction as possible.
- Auditors should review trade integrity and monitoring on a schedule in accordance with its appropriate operational-risk designation.
- Organizations that have customers who trade on margin should establish procedures for collateral valuation and segregated custody accounts.

Fails

In some cases, a bank may not receive or deliver a security by settlement date. "Fails" to deliver for an extended time or a substantial number of cancellations are sometimes characteristic of poor operational control or questionable trading activities.

Fails should be controlled by prompt reporting and follow-up procedures. The use of multicopy confirmation forms enables operational personnel to retain and file a copy by settlement date and should allow for prompt fail reporting and resolution.

Revaluation

The frequency of independent revaluation should be driven by the level of an institution's trading activity. Trading operations with high levels of activity may need to perform daily revaluation; however, it is important to note that independent revaluations are less critical when inventory is turning over quickly or end-of-day positions are small. In these situations, the majority of profit and loss is realized rather than unrealized. Only unrealized profit and loss on positions carried in inventory are affected by a revaluation. At a minimum, every institution should conduct an independent revaluation at the end of each standard accounting period (monthly or quarterly). There will be situations when certain securities will be difficult to price due to lack of liquidity or recent trading activity. If management relies on trader estimates in these situations, a reasonableness test should be performed by personnel who are independent from the trading function. A matrix-pricing approach may also be employed. This involves the use of

prices on similar securities (coupon, credit quality, and tenor) to establish market prices.

Control of Securities

Depository institutions need to adopt procedures to ensure that ownership of securities is adequately documented and controlled. While this documentation and control once involved taking physical possession of the securities either directly or through a third-party custodian, the securities markets are quickly moving to a book-entry system. In this context, safekeeping is more of a concept than a reality. As the markets change, documenting the chain of ownership becomes the primary mechanism to prevent losses arising from a counterparty default. This documentation involves the matching of incoming and outgoing confirmations and frequent reconcilements of all accounts holding securities (Federal Reserve, customer, custodian, and other dealers). When the dealer holds securities on behalf of its customers, similar safeguards also need to be in place. Although this documentation process can be burdensome, it is necessary to protect a dealer's interest in securities owned or controlled. Many active dealers have automated the reconcilement and matching process. This reduces the potential for human error and increases the likelihood that exceptions can be uncovered and resolved quickly.

Because of the relatively short periods of actual ownership associated with repurchase agreements, potential losses could be significant if prudent safeguards are not followed. Significant repo volume or matched-book trading activities only heighten this concern. To further protect their interests, dealers should enter into written agreements with each prospective repurchase-agreement counterparty. Although the industry is moving toward standardized master agreements, some degree of customization may occur. The agreements should be reviewed by legal counsel for their content and compliance with established minimum documentation standards. In general, these agreements should specify the terms of the transaction and the duties of both the buyer and seller. At a minimum, provisions should cover the following issues:

- acceptable types and maturities of collateral securities
- initial acceptable margin for collateral securities of various types and maturities
- margin maintenance, call, default, and sellout provisions
- rights to interest and principal payments
- rights to substitute collateral
- individuals authorized to transact business on behalf of the depository institution and its counterparty

Written agreements should be in place before commencing activities.

TRADING AND CAPITAL-MARKETS ACTIVITIES MANUAL

The *Trading and Capital-Markets Activities Manual*, developed by the Federal Reserve System, is a valuable tool to help examiners understand the complex and often interrelated risks arising from capital-markets activities. The products addressed in the previous subsections and their associated risks are covered in greater detail in the manual.

As noted in the preceding sections, and further addressed in the *Trading and Capital-Markets Activities Manual*, other trading instruments could be included in the bank dealer or money market trading operation. Financial instruments such as futures and forward rate agreements are often used to modify or hedge the risk associated with cash instruments (dealer inventory and money market positions). The bank dealer may also be involved in other instruments including asset-backed securities (mortgage-backed and consumer-receivable-backed). Other departments of the bank may also use securities products as part of an unrelated trading activity. For example, interest-rate-swap traders often use cash bonds to hedge or modify market-risk exposure. In this capacity, the swap desk would be a customer of the government securities dealer. These overlaps in product focus and usage make it critical for examiners to understand the organizational structure and business strategies before establishing examination scope.

OTHER ISSUES

Intercompany Transactions

Examiners should review securities and repurchase-agreement transactions with affiliates to determine compliance with sections 23A and 23B of the Federal Reserve Act. Money market transactions may also be subject to limitations under section 23A; however, these restrictions generally do not apply to transactions between bank subsidiaries that are80 percent or more commonly owned by a bank holding company. Intercompany transactions between securities underwriting affiliates and their bank affiliates should be carefully reviewed to ensure compliance with Board operating standards and sections 23A and 23B.

Agency Relationships

Many dealer banks engage in securities transactions only in an agency capacity. Acting as an agent means meeting customers' investment needs without exposing the firm to the price risk associated with dealing as principal. Risk is relatively low as long as appropriate disclosures are made and the bank does not misrepresent the nature or risk of the security.

Agency-based federal funds transactions are also becoming more common. By serving only as an agent to facilitate the transaction, a bank can meet its correspondent's federal funds needs without inflating the balance sheet and using capital. Examiners should review agency-basedmoney market transactions to ensure that the transactions are structured in a manner that insulates the bank from potential recourse, either moral or contractual. If legal agreements are not structured properly, the courts could conclude that the agent bank was acting a principal. In this situation, the loss could be recognized by the agent bank, not its customer.

Although no single feature can determine whether an agency relationship really exists, the courts have recognized a variety of factors in distinguishing whether the persons to whom "goods" were transferred were buyers or merely agents of the transferor. Although some of these distinguishing factors may not apply to federal-funds transactions because they involve the transfer of funds rather than material goods, some parallels can be drawn. An agency relationship would appear to encompass, although not necessarily be limited to, the following elements:

- The agent bank must agree to act on behalf of the seller of the federal funds ("seller") and not on its own behalf.
- The agent should fully disclose to all parties to the transaction that it is acting as agent on behalf of the seller and not on its own behalf.
- The seller, not the agent bank, must retain title to the federal funds before their sale to a purchasing institution.
- The seller, not the agent bank, must bear the risk of loss associated with the federal-funds sale.
- The agent bank's authority in selling federal funds and accounting for these sales to the seller should be controlled by the seller or by some guidelines to which the seller has agreed. The agent bank should sell only to those banks stipulated on a list of banks approved, reviewed, and confirmed periodically by the seller bank.
- The agent bank should be able to identify the specific parties (sellers and purchasers) to a federal-funds sale and the amount of each transaction for which the agent has acted.
- The agent bank's compensation should generally be based on a predetermined fee schedule or percentage rate (for example, a percentage based on the number or size of transactions). The agent should generally not receive compensation in the form of a spread over a predetermined rate that it pays to the seller. (If the agent bank's compensation is in the form of a spread over the rate it pays to the seller, this situation would appear to be more analogous to acting as a principal and suggests that the transactions should be reported on the "agent's" balance sheet.)

By structuring agency agreements to include provisions that encompass these factors and by conducting agency activities accordingly, agent banks can lower the possibility that they would be considered a principal in the event of a failure of a financial institution that had purchased funds through the agent. Generally, as a matter of prudent practice, each bank acting as an agent should have written agreements with principals encompassing the above elements and have a written opinion from legal counsel as to the bona fide nature of the agency relationships.

Selling through an agent should not cause a bank to neglect a credit evaluation of the ultimate purchasers of these funds. Under the more traditional mode of conducting federal-funds transactions, banks sell their federal funds to other banks, which in many instances are larger regional correspondents. These correspondent banks in turn may resell the federal funds to other institutions. Since the correspondent is acting as a principal in these sales, the banks selling the funds to the correspondent are generally not concerned about the creditworthiness of those purchasing the federal funds from the correspondent/principal. Rather, the original selling banks need to focus solely on the creditworthiness of their correspondent banks, with which they should be quite familiar.

However, when conducting federal-funds sales through an agent, selling banks, in addition to considering the financial condition of their agent, should also subject the ultimate purchasing banks to the same type of credit analysis that would be considered reasonable and prudent if the seller banks were lending directly to the ultimate borrowers rather than through agents. Banks selling federal funds through agents should not relinquish their credit-evaluation responsibilities to their agent banks.

REPORTING

Securities held for trading purposes and the income and expense that results from trading activities should be isolated by specific general ledger or journal accounts. The balances in those accounts should be included in the appropriate reporting categories for regulatory reporting.

Instructions for the Consolidated Report of Condition and Income (call report) require that securities, derivative contracts, and other items held in trading accounts be reported consistently at market value, or at the lower of cost or market value, with unrealized gains and losses recognized in current income. For further detail, refer to the glossary section of the call report instructions under ''trading account.'' With either method, the carrying values of trading-security inventories should be evaluated periodically (monthly or quarterly), based on current market prices. The increase or decrease in unrealized appreciation or depreciation resulting from that revaluation should be credited or charged to income. Periodic independent revaluation is the most effective means of measuring the trading decisions of bank management.

For reporting purposes, the trading department's income should include not only revaluation adjustments, but also profits and losses from the sale of securities, and other items related to the purchase and sale of trading securities. Interest income from trading assets, salaries, commissions, and other expenses should be excluded from trading income for reporting purposes; however, these items should be considered by management when evaluating the overall profitability of the business.

When the lender institution is acting as a fully disclosed agent, securities-lending activities need not be reported on the call report. However, lending institutions offering indemnification against loss to their customer-owners should report the associated contingent liability gross in Schedule RC-L as "other significant commitments and contingencies."

Recordkeeping and Confirmation Rules

Regulation H contains rules establishing uniform standards for bank recordkeeping, confirmation, and other procedures in executing securities transactions for bank customers. The regulation applies, in general, to those retail commercial activities where the bank effects securities transactions at the direction and for the account of customers. The purpose of the rules is to ensure that purchasers of securities are provided adequate information concerning a transaction and that adequate records and controls are maintained for securities transactions. Under the rules, banks are required to maintain certain detailed records concerning securities transactions, to provide written confirmations to customers under certain circumstances, and to establish certain written policies and procedures. The requirements generally do not apply to banks that make 200 or fewer securities transactions a year for customers (exclusive of transactions in U.S. government and agency obligations) and to transactions subject to the requirements of the MSRB.

Due Bills

A "due bill" is an obligation that results when a firm sells a security or money market instrument and receives payment, but does not deliver the item sold. Due bills issued should be considered as borrowings by the issuing firm, and alternatively, due bills received should be considered as lending transactions. Dealers should not issue due bills as a means of obtaining operating funds or when the underlying security can be delivered at settlement. Customers of the dealer enter transactions with an implicit understanding that securities transactions will be promptly executed and settled unless there is a clear understanding to the contrary. Consequently, dealers should promptly disclose the issuance of a due bill to a customer when funds are taken but securities or money market instruments are not delivered to the customer. Such disclosure should reference the applicable transaction; state the reason for the creation of a due bill; describe any collateral securing the due bill; and indicate that to the extent the market value of the collateral is insufficient, the customer may be an unsecured creditor of the dealer.

Due bills that are outstanding for more than three days and are unsecured could be construed as funding and should be reported as "liabilities for borrowed monies" on the call report. These balances are subject to reserve requirements imposed by Regulation D.

ESTABLISHING SCOPE

Obtaining an overview of the organization, management structure, products offered, and control environment is a critical step in the examination process. Based on this assessment, an examiner should determine the appropriate resources and skill level. In situations where an institution is active in either the government or municipal securities markets, it is essential to allocate additional resources for GSA and MSRB compliance. The assigned examiners should be familiar with the provisions of GSA and MSRB as well as with the related examination procedures. For active proprietary trading units, it is important to assign examiners who have a reasonable working knowledge of the concepts outlined in the *Trading Activities Manual*.

1. To determine if the policies, practices, procedures, and internal controls regarding bank dealer activities are adequate.
2. To determine if bank officers are operating in conformance with the established guidelines.
3. To evaluate the trading portfolio for credit quality and marketability.
4. To determine the scope and adequacy of the audit compliance functions.
5. To determine compliance with applicable laws and regulations.
6. To ensure investor protection.
7. To initiate corrective action when policies, practices, procedures, or internal controls are deficient or when violations of law or regulations have been noted.

1. If selected for implementation, complete or update the Bank Dealer Activities 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. 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 corrections have been accomplished.
4. Request that the bank provide the following schedules:
   a. An aged schedule of securities that have been acquired as a result of underwriting activities.
   b. An aged schedule of trading account securities and money market instruments held for trading or arbitrage purposes. Reflect commitments to purchase and sell securities and all joint account interests.
   c. A schedule of short-sale transactions.
   d. An aged schedule of due bills.
   e. A list of bonds borrowed.
   f. An aged schedule of "fails" to receive or deliver securities on unsettled contracts.
   g. A schedule of approved securities borrowers and approved limits.
   h. A schedule of loaned securities.
   i. A schedule detailing account names and/or account numbers of the following customer accounts:
      - Own bank trust accounts.
      - Own bank permanent portfolio.
      - Affiliated banks' permanent portfolio accounts.
      - Personal accounts of employees of other banks.
      - Accounts of brokers or other dealers.
      - Personal accounts of employees of other brokers or dealers.
   j. A list of all joint accounts entered into since the last examination.
   k. A list of underwriting since the last examination and whether such securities were acquired by negotiation or competitive bid.
   l. A list of all financial advisory relationships.
5. Agree balances of appropriate schedules to general ledger and review reconciling items for reasonableness.
6. Determine the extent and effectiveness of trading policy supervision by:
   a. Reviewing the abstracted minutes of meetings of the board of directors and/or of any appropriate committee.
   b. Determining that proper authorization for the trading officer or committee has been made.
   c. Ascertaining the limitations or restrictions on delegated authorities.
   d. Evaluating the sufficiency of analytical data used in the most recent board or committee trading department review.
   e. Reviewing the methods of reporting by department supervisors and internal auditors to ensure compliance with established policy and law.
   f. Reaching a conclusion about the effectiveness of director supervision of the bank's trading policy. Prepare a memo for the examiner assigned "Duties and Responsibilities of Directors" stating your conclusions. All conclusions should be supported by factual documentation.

   (Before continuing, refer to steps 14 and 15. They should be performed in conjunction with the remaining examination steps.)

7. Ascertain the general character of underwriting and direct placement activities and the effectiveness of department management by reviewing underwriter files and ledgers, committee reports and offering statements to determine:
   a. The significance of underwriting activities and direct placements of type III securities as reflected by the volume of sales and profit or loss on operations. Compare current data to comparable prior periods.
   b. Whether there is a recognizable pattern in:

- The extent of analysis of materialinformation relating to the ability of the issuer to service the obligation.
- Rated quality of offerings.
- Point spread of profit margin for unrated issues.
- Geographic distribution of issuers.
- Syndicate participants.
- Bank's trust department serving as corporate trustee, paying agent and transfer agent for issuers.
- Trustee, paying agent and transfer agent business being placed with institutions that purchase a significant percentage of the underwriter or private placement offering.

c. The volume of outstanding bids. Compare current data to comparable prior periods.
d. The maturity, rated quality and geographic distribution of takedowns from syndicate participations.
e. The extent of transfer to the bank's own or affiliated investment or trading portfolios or to trust accounts and any policies relating to this practice.

8. Determine the general character of trading account activities and whether the activities are in conformance with stated policy by reviewing departmental reports, budgets and position records for various categories of trading activity and determining:
   a. The significance of present sales volume compared to comparable prior periods and departmental budgets.
   b. Whether the bank's objectives are compatible with the volume of trading activity.
9. Review customer ledgers, securities position ledgers, transaction or purchase and sales journals and analyze the soundness of the bank's trading practices by:
   a. Reviewing a representative sample of agency and contemporaneous principal trades and determining the commission and price mark-up parameters for various sizes and types of transactions.
   b. Selecting principal transactions that have resulted in large profits and determining if the transaction involved:
      - ''Buy-backs'' of previously traded securities.
      - Own bank or affiliated bank portfolios.
      - A security that has unusual quality and maturity characteristics.

   c. Reviewing significant inventory positions taken since the prior examination and determining if:
      - The quality and maturity of the inventory position was compatible with prudent banking practices.
      - The size of the position was within prescribed limits and compatible with a sound trading strategy.

   d. Determining the bank's exposure on offsetting repurchase transactions by:
      - Reviewing the maturities of offsetting re-po and reverse re-po agreements to ascertain the existence, duration, amounts and strategy used to manage unmatched maturity ''gaps'' and extended (over 30 days) maturities.
      - Reviewing records since the last examination to determine the aggregate amounts of:
        — Matched repurchase transactions.
        — Reverse re-po financing extended to one or related firms(s).
      - Performing credit analysis of significant concentrations with any single or related entity(ies).
      - Reporting the relationship of those concentrations to the examiners assigned ''Concentration of Credits'' and ''Funds Management.''
10. Determine the extent of risk inherent in trading account securities which have been in inventory in excess of 30 days and:
    a. Determine the dollar volume in extended holdings.
    b. Determine the amounts of identifiable positions with regard to issue, issuer, yield, credit rating, and maturity.
    c. Determine the current market value for individual issues which show an internal valuation mark-down of 10 percent or more.
    d. Perform credit analyses on the issuers of non-rated holdings identified as significant positions.
    e. Perform credit analyses on those issues with valuation write-downs considered significant relative to the scope of trading operations.
    f. Discuss plans for disposal of slow moving inventories with management and determine the reasonableness of those plans in light of current and projected market trends.

11. Using an appropriate technique, select issuesfrom the schedule of trading account inventory. Test valuation procedures by:
    a. Reviewing operating procedures and supporting workpapers and determining if prescribed valuation procedures are being followed.
    b. Comparing bank prepared market prices, as of the most recent valuation date, to an independent pricing source (use trade date "bid" prices).
    c. Investigating any price differences noted.
12. Using an appropriate technique, select transactions from the schedule of short sales and determine:
    a. The degree of speculation reflected by basis point spreads.
    b. Present exposure shown by computing the cost to cover short sales.
    c. If transactions are reversed in a reasonable period of time.
    d. If the bank makes significant use of due-bill transactions to obtain funds for its banking business:
        • Coordinate with the examiner assigned "Review of Regulatory Reports" to determine if the bank's reports of condition reflect due bill transactions as "liabilities for borrowed money."
        • Report amounts, duration, seasonal patterns and budgeted projections for due bills to the examiner assigned "Funds Management."
13. If the bank is involved in agency-based federal funds activity:
    a. At the beginning or in advance of each examination of a banking organization which has been acting as an agent in the purchase and sale of federal funds for other institutions, examiners should obtain certain information which will help them determine the nature and extent of this activity. The information should include:
        • A brief description of the various types of agency relationships (i.e., involving federal funds or other money market activities) and the related transactions.
        • For each type of agency relationship, copies of associated forms, agency agreements, documents, reports and legal opinions. In addition, if the banking organization has documented its analysis of the risks associated with the activity, a copy of the analysis should be requested by the examiner.
        • For each type of agency relationship, a summary of the extent of the activity including:
            — The number of institutions serviced as principals.
            — The size range of the institutions (i.e., institutions serviced have total assets ranging from $_____ to $_____).
            — General location of sellers and purchasers serviced under agency relationships (i.e., New York State, Midwest, etc.)
            — Estimate of average daily volume of federal funds or money market instruments purchased and sold under agency relationships and the high and low volume over the period since the last examination inquiry (or since activity was begun, if more recent).
            — Names of individuals in the bank that are responsible for these agency relationships.
        • A historical file of this information should be maintained in order to determine the nature, extent and growth of these activities over time.
    b. Once the examination work in this area has been started, the examiner should attempt to discern any situation, activity or deficiency in this area that might suggest that an agency relationship does *not* actually exist. A negative response to the following examination guidelines section dealing with agency agreements may signal such a deficiency. In addition, any other money market agency relationships that involve new or unusual financial transactions should be evaluated to determine the nature of the risks involved and compliance, to the extent applicable, with the guidelines.
    c. The examiner should determine that the banking organization's written policies, procedures, and other documentation associated with this activity are consistent with the Federal Reserve System's Examination Guidelines. If the bank does not have written policies the examiner should strongly advise that they be developed due to the complex nature of

this activity and the potential risks associated with it.

d. After reviewing the policies, procedures, and appropriate documentation, the examiner should be able to respond positively to the following questions:
   - Banking organizations acting as *agents in the sale of federal funds*[1]
     — Has this form of activity been approved by the board of directors?
     — Are the bank's individual agency arrangements and transactions:
       - supported by written agency agreements, and
       - reviewed and approved by appropriate officers?
     — Do the written agency agreements that support this activity include provisions indicating that (a negative answer may indicate that the bank is not in fact an agent):
       - the agent bank will be acting *on behalf of the original or principal seller of federal funds ("seller")* in conducting these activities and not on the agent bank's own behalf?
       - the agency relationship will be fully disclosed to all banks involved in the transactions?
       - the seller, and not the agent bank, must retain legal title to the federal funds before they are sold to a third party bank?
       - the seller, and not the agent bank, bears the risk of loss?
       - the agent bank's authority in selling federal funds and in accounting for this activity to the seller should be controlled by the seller or by standards to which it has agreed? To implement this, does the agreement or its attachments include the following seller-approved items:
         1. lists of banks to whom the agent may sell federal funds,[2] and
         2. limits on the amounts that can be sold to these banks?
     — Does the agent have a written opinion from its legal counsel as to the bona fide nature of the agency relationship?
     — Does the accounting and reporting system of the agent bank *enable* it to account for the federal funds transactions on a period basis (i.e., at least weekly) to the sellers? (Although more frequent accounting may not be required by the sellers, the agent on any day should have the capacity to identify for the seller the banks to whom the seller's funds have been sold.)
     — Does the agent's accounting system identify *each bank* which has purchased federal funds from a particular seller bank and include (at least) the following information for *each bank* in which the funds are being invested?[3]
       - information to clearly identify the name and location of the bank (or other entity)
       - amount of federal funds sold and amount of interest earned
       - terms of transaction, and maturity date
       - lending limits agreed to
     — Does the agent bank actually disclose to banks or other organizations that are part of these agency-based transactions that it is acting as agent?
     — Is the agent bank's compensation in the form of a predetermined fee schedule or percentage rate based, for example, on the size of transactions, as opposed to compensation in the form of a spread over the rate that it pays to the seller bank? (If the agent bank's compen-

1. Although it is conceivable that a purchaser could engage an agent to *obtain* federal funds on its behalf, these guidelines focus primarily on situations where the seller has engaged an agent to sell federal funds on its behalf because the associated risks of such transactions are borne by the sellers and their agents.

2. Seller banks could conceivably design their lists of approved banks to encompass a large number of financially sound institutions and still be considered to be fulfilling this supervisory requirement.

3. The entities referred to as "ultimate purchasers" or "ultimate borrowers" are those that have the *responsibility to repay* the original seller bank, and not any intervening agents that may pass on the federal funds to these purchasers.

sation is in the form of a spread over the rate it pays to the selling bank, this situation would appear to be more akin to acting as an intermediary and suggests that the transactions should be reported on its balance sheet.)

- Banking organizations that are involved in agency-based federal funds relationships as *sellers*
  - — Does the bank support its transactions with written agency agreements?
  - — Does the seller bank evaluate the credit worthiness of the ultimate borrowers of federal funds and establish limits for each and are these limits periodically reviewed at least every six months?[3,4]
  - — Does the bank periodically (i.e., at least weekly) receive an accounting from the agent which includes the following information for *each bank* to whom the seller bank's federal funds were sold?
    - information to identify name and location of bank
    - amount of federal funds sold and interest earned
    - federal funds sales limits agreed to (if the seller bank is a principal)
  - — Is the bank's management and board of directors aware of and have they approved the agency relationship?
- Do internal and/or external auditors periodically review the policies, procedures, and internal controls associated with this activity and the activity's impact on the earnings and financial condition of the banking organization? Is their evaluation reported to management? (Applies to banks acting as *agents* in the sale of federal funds, *and* those banks involved as *sellers* of federal funds.)
- In addition to the items considered above, the examiner should determine what the impact of these transactions has been on the bank's earnings and financial condition. If the impact has been negative, or if the answer to any of the above questions is negative, the examiner should discuss these matters with bank management and seek remedial action.

14. Analyze the effectiveness of operational controls by reviewing recent cancellations and fail items that are a week or more beyond settlement date and determine:
    a. The amount of extended fails.
    b. The planned disposition of extended fails.
    c. If the control system allows a timely, productive follow-up on unresolved fails.
    d. The reasons for cancellations.
    e. The planned disposition of securities that have been inventoried prior to the recognition of a fail or a cancellation.
15. Determine compliance with applicable laws, rulings, and regulations by performing the following for:
    a. *12 CFR 1.3—Eligible Securities:*
       - Review inventory schedules of underwriting and trading accounts and determine if issues whose par value is in excess of 10 percent of the bank's captial and unimpaired surplus are type I securities.
       - Determine that the total par value of type II investments does not exceed 10 percent of the bank's capital and unimpaired surplus, based on the combination of holdings and permanent portfolio positions in the same securities.
       - Elicit management's comments and review underwriting records on direct placement of type III securities, and determine if the bank is dealing in type III securities for its own account by ascertaining if direct placement issues have been placed in own bank or affiliated investment portfolios or if underwriting proceeds were used to reduce affiliate loans.
    b. *Section 23A of the Federal Reserve Act (12 USC 371(c) and 375)—Preferential Treatment:* Obtain a list of domestic affiliate relationships and a list of directors and principal officers and their business interests from appropriate examiners and determine whether transactions, include securities clearance services, involving affiliates, insiders or their

4. This requirement is intended to mean that seller banks should conduct the type of credit analysis that would be considered reasonable and prudent for a direct federal funds activity (i.e., those federal funds activities not conducted through agents).

interests are on terms less favorable to the bank than those transactions involving unrelated parties.

c. *Regulation D (12 CFR 204.2)—Due Bills:*
   - Review outstanding due bills and determine if:
     — The customer was informed that a due bill would be issued instead of the purchased security.
     — Safekeeping receipts are sent to safekeeping customers only after the purchased security has been delivered.
   - Review due bills outstanding over three business days and determine if they are collateralized or properly reserved.
   - Review collateralized due bills and determine if the liability is secured by securities of the same type and of comparable maturity and with a market value at least equal to that of the security that is the subject of the due bill.

d. *Regulation H (12 CFR 208.8(k))—Recordkeeping and Confirmation Requirements:* If the bank effects securities transactions at the direction and for the account of customers, determine if it is in compliance with this regulation by substantiating Internal Control questions 24–35.

16. Test for unsafe and unsound practices and possible violations of the Securities Exchange Act of 1934 by:
    a. Reviewing customer account schedules of own bank and affiliated bank permanent portfolios, trusts, other broker-dealers, employees of own or other banks and other broker-dealers. Use an appropriate technique to select transactions and compare trade prices to independently established market prices as of the date of trade.
    b. Reviewing transactions, including U.S. government tender offer subscription files, involving employees and directors of own or other banks and determine if the funds used in the transactions were misused bank funds or the proceeds of reciprocal or preferential loans.
    c. Reviewing sales to affiliated companies to determine that the sold securities were not subsequently repurchased at an additional mark-up and that gains were not recognized a second time.
    d. Reviewing commercial paper sales journals or confirmations to determine if the bank sells affiliate commercial paper. If so, determine if:
       - The bank sells affiliate-issued commercial paper to institutions and financially sophisticated individuals only.
       - Sales are generally denominated in amounts of $25,000 or more.
       - Each sale confirmation discloses that the affiliate-issued commercial paper is not an insured bank deposit.
    e. Reviewing securities position records and customer ledgers with respect to large volume repetitive purchase and sales transactions and:
       - Independently testing market prices of significant transactions which involve the purchase and resale of the same security to the same or related parties.
       - Investigating the purchase of large blocks of securities from dealer firms just prior to month end and their subsequent resale to the same firm just after the beginning of the next month.
    f. Reviewing lists of approved dealer firms and determining that the approval of any firm that handles a significant volume of agency transactions is based on competitive factors rather than deposit relationships.
    g. Reviewing customer complaint files and determining the reasons for such complaints.
17. Discuss with an appropriate officer and prepare report comments concerning:
    a. The soundness of trading objectives, policies and practices.
    b. The degree of legal and market risk assumed by trading operations.
    c. The effectiveness of analytical, reporting and control systems.
    d. Violations of law.
    e. Internal control deficiencies.
    f. Apparent or potential conflicts of interest.
    g. Other matters of significance.
18. Reach a conclusion regarding the quality of department management and state your conclusions on the management brief provided by the examiner assigned "Management Assessment."
19. Update workpapers with any information that will facilitate future examinations.

Review the bank's internal controls, policies, practices and procedures regarding bank dealer activities. The bank's system should be documented in a complete, 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.

This section applies to all bank dealer activities except those involving municipal securities, which are reviewed as part of a separate and distinct Municipal Bond Dealer Examination.

SECURITIES UNDERWRITING TRADING POLICIES

1. Has the board of directors, consistent with its duties and responsibilities, adopted written securities underwriting/trading policies that:
   a. Outline objectives?
   b. Establish limits and/or guidelines for:
      - Price mark-ups?
      - Quality of issues?
      - Maturity of issues?
      - Inventory positions (including when issued (WI) positions)?
      - Amounts of unrealized loss on inventory positions?
      - Length of time an issue will be carried in inventory?
      - Amounts of individual trades or underwriter interests?
      - Acceptability of brokers and syndicate partners?
   c. Recognize possible conflicts of interest and establish appropriate procedures regarding:
      - Deposit and service relationships with municipalities whose issues have underwriting links to the trading department?
      - Deposit relationships with securities firms handling significant volumes of agency transactions or syndicate participations?
      - Transfers made between trading account inventory and investment portfolio(s)?
      - The bank's trust department acting as trustee, paying agent, and transfer agent for issues which have an underwriting relationship with the trading department?
   d. State procedures for periodic, monthly or quarterly, valuation of trading inventories to market value or to the lower of cost or market price?
   e. State procedures for periodic independent verification of valuations of the trading inventories?
   f. Outline methods of internal review and reporting by department supervisors and internal auditors to insure compliance with established policy?
   g. Identify permissible types of securities?
   h. Ensure compliance with the rules of fair practice that:
      - Prohibit any deceptive, dishonest or unfair practice?
      - Adopt formal suitability checklists?
      - Monitor gifts and gratuities?
      - Prohibit materially false or misleading advertisements?
      - Adopt a system to determine the existence of possible control relationships?
      - Prohibit the use of confidential, nonpublic information without written approval of the affected parties?
      - Prohibit improper use of funds held on another's behalf?
      - Allocate responsibility for transactions with own employees and employees of other dealers?
      - Require disclosure on all new issues?
   i. Provide for exceptions to standard policy?
2. Are the underwriting/trading policies reviewed at least quarterly by the board to determine their adequacy in light of changing conditions?
3. Is there a periodic review by the board to assure that the underwriting/trading department is in compliance with its policies?

OFFSETTING RESALE AND REPURCHASE TRANSACTIONS

4. Has the board of directors, consistent with its duties and responsibilities, adopted written offsetting repurchase transaction policies that:
   a. Limit the aggregate amount of offsetting repurchase transactions?
   b. Limit the amounts in unmatched or extended (over 30 days) maturity transactions?
   c. Determine maximum time gaps for unmatched maturity transactions?
   d. Determine minimumly acceptable interest rate spreads for various maturity transactions.
   e. Determine the maximum amount of funds to be extended to any single or related firms through reverse re-po transactions, involving unsold (through forward sales) securities?
   f. Require firms involved in reverse re-po transactions to submit corporate resolutions stating the names and limits of individuals, who are authorized to commit the firm?
   g. Require submission of current financial information by firms involved in reverse re-po transactions?
   h. Provide for periodic credit reviews and approvals for firms involved in reverse re-po transactions?
   i. Specify types of acceptable offsetting repurchase transaction collateral (if so, indicate type _____).
5. Are written collateral control procedures designed so that:
   a. Collateral assignment forms are used?
   b. Collateral assignments of registered securities are accompanied by powers of attorney signed by the registered owner?
      • Registered securities are registered in bank or bank's nominee name when they are assigned as collateral for extended maturity (over 30 days) reverse re-po transactions?
   c. Funds are not disbursed until reverse re-po collateral is delivered into the physical custody of the bank or an independent safekeeping agent?
   d. Funds are only advanced against predetermined collateral margins ordiscounts?
      • If so, indicate margin or discount percentage _____.
   e. Collateral margins or discounts are predicated upon:
      • The type of security pledged as collateral?
      • Maturity of collateral?
      • Historic and anticipated price volatility of the collateral?
      • Maturity of the reverse re-po agreements?
   f. Maintenance agreements are required to support predetermined collateral margin or discount?
   g. Maintenance agreements are structured to allow margin calls in the event of collateral price declines?
   h. Collateral market value is frequently checked to determine compliance with margin and maintenance requirements (if so, indicate frequency _____)?

CUSTODY AND MOVEMENT OF SECURITIES

*6. Are the bank's procedures such that persons do not have sole custody of securities in that:
   a. They do not have sole physical access to securities?
   b. They do not prepare disposal documents that are not also approved by authorized persons?
   c. For the security custodian, supporting disposal documents are examined or adequately tested by a second custodian?
   d. No person authorizes more than one of the following transactions: execution of trades, receipt and delivery of securities, and collection or disbursement of payment?
7. Are securities physically safeguarded to prevent loss, unauthorized disposal or use? And:
   a. Are negotiable securities kept under dual control?
   b. Are securities counted frequently, on a surprise basis, reconciled to the securi-

ties record, and the results of such counts reported to management?

c. Does the bank periodically test for compliance with provisions of its insurance policies regarding custody of securities?

d. For securities in the custody of others:
- Are custody statements agreed periodically to position ledgers and any differences followed up to a conclusion?
- Are statements received from brokers and other dealers reconciled promptly, and any differences followed up to a conclusion?
- Are positions for which no statements are received confirmed periodically, and stale items followed up to a conclusion?

8. Are trading account securities segregated from other bank owned securities or securities held in safekeeping for customers?

*9. Is access to the trading securities vault restricted to authorized employees?

10. Do withdrawal authorizations require countersignature to indicate security count verifications?

11. Is registered mail used for mailing securities, and are adequate receipt files maintained for such mailings (if registered mail is used for some but not all mailings, indicate criteria and reasons)?

12. Are prenumbered forms used to control securities trades, movements and payments?

13. If so, is numerical control of prenumbered forms accounted for periodically by persons independent of those activities?

14. Do alterations to forms governing the trade, movement, and payment of securities require:

*a. Signature of the authorizing party?

b. Use of a change of instruction form?

15. With respect to negotiability of registered securities:

a. Are securities kept in non-negotiable form whenever possible?

b. Are all securities received, and not immediately delivered, transferred to the name of the bank or its nominee and kept in non-negotiable form whenever possible?

c. Are securities received checked for negotiability (endorsements, signature, guarantee, legal opinion, etc.) and for completeness (coupons, warrants, etc.) before they are placed in the vault?

RECORDS MAINTENANCE

16. Does the bank maintain:

a. Order tickets which include:
- Capacity as principal or agent?
- If order is firm or conditional?
- Terms, conditions or instructions and modifications?
- Type of transaction (purchase or sale)?
- Execution price?
- Description of security?
- Date and time of order receipt?
- Date and time of execution?
- Dealer's or customer's name?
- Delivery and payment instructions?
- Terms, conditions, date and time of cancellation of an agency order?

b. Customer confirmations:
- Bank dealer's name, address and phone number?
- Customer's name?
- Designation of whether transaction was a purchase from or sale to the customer?
- Par value of securities?
- Description of securities, including at a minimum:
  - — Name of issuer?
  - — Interest rate?
  - — Maturity date?
  - — Designation, if securities are subject to limited tax?
  - — Subject to redemption prior to maturity (callable)?
  - — Designation, if revenue bonds and the type of revenue?
  - — The name of any company or person in addition to the issuer who is obligated, directly or indirectly, to pay debt service on revenue bonds? (In the case of more than one such obligor, the phrase "multiple obligors" will suffice.)
  - — Dated date, if it affects price or interest calculations?
  - — First interest payment date, if other than semi-annual?

— Designation, if securities are "fully registered" or "registered as principal"?
— Designation, if securities are "pre-refunded"?
— Designation, if securities have been "called," maturity date fixed by call notice and amount of call price?
— Denominations of bearer bonds, if other than denominations of $1,000 and $5,000 par value?
— Denominations of registered bonds, if other than multiples of $1,000 par value up to $100,000 par value?
— Denominations of municipal notes?

- Trade date and time of execution, or a statement that time of execution will be furnished upon written request of the customer?
- Settlement date?
- Yield and dollar price? Only the dollar price need to be shown for securities traded at par.
  — For transactions in callable securities effected on a yield basis, the resulting price calculated to the lowest of price to call premium, par option (callable at par) or to maturity, and if priced to premium call or par option, a statement to that effect and the call or option date and price used in the calculation?
- Amount of accrued interest?
- Extended principal amount?
- Total dollar amount of transaction?
- The capacity in which the bank dealer effected the transaction:
  — As principal for own account?
  — As agent for customer?
  — As agent for a person other than the customer?
  — As agent for both the customer and another person (dual agent)?
- If a transaction is effected as agent for the customer or as dual agent:
  — Either the name of the contra-party or a statement that the information will be furnished upon request?
  — The source and amount of any commission or other remuneration to the bank dealer?
- Payment and delivery instructions?
- Special instructions, such as:
  — "Ex-legal" (traded without legal opinion)?
  — "Flat" (traded without interest)?
  — "In default" as to principal or interest?

c. Dealer confirmations:
- Bank dealer's name, address and telephone number?
- Contra-party identification?
- Designation of purchase from or sale to?
- Par value of securities?
- Description of securities, including at a minimum:
  — Name of issuer?
  — Interest rate?
  — Maturity date?
  — Designation, if securities are limited tax?
  — Subject to redemption prior to maturity (callable)?
  — Designation, if revenue bonds and the type of revenue?
  — Dated date, if it affects price or interest calculations?
  — First interest payment date, if other than semi-annual?
  — Designation, if securities are "fully registered" or "registered as principal"?
  — Designation, if securities are "pre-refunded"?
  — Designation, if securities have been "called," maturity date fixed by call notice and amount of call price?
  — Denominations of bearer bonds, if other than denominations of $1,000 and $5,000 par value?
  — Denominations of registered bonds, if other than multiples of $1,000 par value up to $100,000 par value?
- CUSIP number, if assigned (effective January 1, 1979)?
- Trade date?
- Settlement date?
- Yield to maturity and resulting dollar price? Only the dollar price need be

shown for securities traded at par or on a dollar basis.
  - — For transactions in callable securities effected on a yield basis, the resulting price calculated to the lowest of price to call premium, par option (callable at par) or to maturity?
  - — If applicable, the fact that securities are priced to premium call or par option and the call or option date and price used in the calculation?
- Amount of accrued interest?
- Extended principal amount?
- Total dollar amount of transaction?
- Payment and delivery instructions?
- Special instructions, such as:
  - — "Ex-legal" (traded without legal opinion)?
  - — "Flat" (traded without interest)?
  - — "In default" as to principal or interest?

d. Purchase and sale journals or blotters which include:
- Trade date?
- Description of securities?
- Aggregate par value?
- Unit dollar price or yield?
- Aggregate trade price?
- Accrued interest?
- Name of buyer or seller?
- Name of party received from or delivered to?
- Bond or note numbers?
- Indication if securities are in registered form?
- Receipts or disbursements of cash?
- Specific designation of "when issued" transactions?
- Transaction or confirmation numbers recorded in consecutive sequence to insure that transactions are not omitted?
- Other references to documents of original entry?

e. Short sale ledgers which include:
- Sale price?
- Settlement date?
- Present market value?
- Basis point spread?
- Description of collateral?
- Cost of collateral or cost to acquire collateral?
- Carrying charges?

f. Security position ledgers, showing separately for each security positioned for the bank's own account:
- Description of the security?
- Posting date (either trade or settlement date, provided posting date is consistent with other records of original entry)?
- Aggregate par value?
- Cost?
- Average cost?
- Location?
- Count differences classified by the date on which they were discovered?

g. Securities transfer or validation ledgers which include:
- Address where securities were sent?
- Date sent?
- Description of security?
- Aggregate par value?
- If registered securities:
  - — Present name of record?
  - — New name to be registered?
- Old certificate or note numbers?
- New certificate or note numbers?
- Date returned?

h. Securities received and delivered journals or tickets which include:
- Date of receipt or delivery?
- Name of sender and receiver?
- Description of security?
- Aggregate par value?
- Trade and settlement dates?
- Certificate numbers?

i. Cash or wire transfer receipt and disbursement tickets which include:
- Draft or check numbers?
- Customer accounts debited or credited?
- Notation of the original entry item that initiated the transaction?

j. Cash or wire transfer journals which additionally include:
- Draft or check reconcilements?
- Daily totals of cash debits and credits?
- Daily proofs?

k. Fail ledgers which include:
- Description of security?
- Aggregate par value?
- Price?
- Fail date?
- Date included on fail ledger?
- Customer or dealer name?
- Resolution date?

- A distinction between a customer and a dealer fail?
- Follow-up detail regarding efforts to resolve the fail?

l. Securities borrowed and loaned ledgers which include:
- Date of transaction?
- Description of securities?
- Aggregate par value?
- Market value of securities?
- Contra-party name?
- Value at which security was loaned?
- Date returned?
- Description of collateral?
- Aggregate par value of collateral?
- Market value of collateral?
- Collateral safekeeping location?
- Dates of periodic valuations?

m. Records concerning written or oral put options, guarantee and repurchase agreements which include:
- Description of the securities?
- Aggregate par value?
- Terms and conditions of the option, agreement or guarantee?

n. Customer account information which includes:
- Customer's name and residence or principal business address?
- Whether customer is of legal age?
- Occupation?
- Name and address of employer? And:
  — Whether customer is employed by a securities broker or dealer or by a municipal securities dealer?
- Name and address of beneficial owner or owners of the account if other than customer? And:
  — Whether transactions are confirmed with such owner or owners?
- Name and address of person(s) authorized to transact business for a corporate, partnership or trusteed account? And:
  — Copy of powers of attorney, resolutions or other evidence of authority to effect transactions for such an account?
- With respect to borrowing or pledging securities held for the accounts of customers:
  — Written authorization from the customer authorizing such activities?
- Customer complaints including:
  — Records of all written customer complaints?
  — Record of actions taken concerning those complaints?

o. Customer and the bank dealer's own account ledgers which include:
- All purchases and sales of securities?
- All receipts and deliveries of securities?
- All receipts and disbursements of cash?
- All other charges or credits?

p. Records of syndicates' joint accounts or similar accounts formed for the purchase of municipal securities which include:
- Underwriter agreements? And:
  — Description of the security?
  — Aggregate par value of the issue?
- Syndicate or selling group agreements? And:
  — Participants' names and percentages of interest?
  — Terms and conditions governing the formation and operation of the syndicate?
  — Date of closing of the syndicate account?
  — Reconcilement of syndicate profits and expenses?
- Additional requirements for syndicate or underwriting managers which include:
  — All orders received for the purchase of securities from the syndicate or account, except bids at other than the syndicate price?
  — All allotments of securities and the price at which sold?
  — Date of settlement with the issuer?
  — Date and amount of any good faith deposit made with the issuer?

q. Files which include:
- Advertising and sales literature
- Prospectus delivery information?

r. Internal supervisory records which include:
- Account reconcilement and follow-up?
- Profit analysis by trader?
- Sales production reports?

- Periodic open position reports computed on a trade date or when issued basis?
- Reports of own bank credit extensions used to finance the sale of trading account securities?

PURCHASE AND SALES TRANSACTIONS

17. Are all transactions promptly confirmed in writing to the actual customers or dealers?
18. Are confirmations compared or adequately tested to purchase and sales memoranda and reports of execution of orders, and any differences investigated and corrected (including approval by a designated responsible employee)?
    a. Are confirmations and purchase and sale memoranda checked or adequately tested for computation and terms by a second individual?
19. Are comparisons received from other dealers or brokers compared with confirmations, and any differences promptly investigated?
    a. Are comparisons approved by a designated individual (if so, give name _____)?

CUSTOMER AND DEALER ACCOUNTS

20. Do account bookkeepers periodically transfer to different account sections or otherwise rotate posting assignments?
21. Are letters mailed to customers requesting confirmation of changes of address?
22. Are separate customer account ledgers maintained for:
    - Employees?
    - Affiliates?
    - Own bank's trust accounts?
23. Are customer inquiries and complaints handled exclusively by designated individuals who have no incompatible duties?

RECORDKEEPING AND CONFIRMATION REQUIREMENTS FOR CUSTOMER SECURITIES TRANSACTIONS (REGULATION H)

24. Are chronological records of original entry containing an itemized daily record of all purchases and sales of securities maintained?
25. Do the original entry records reflect:
    a. The account or customer for which each such transaction was effected?
    b. The description of the securities?
    c. The unit and aggregate purchase or sale price (if any)?
    d. The trade date?
    e. The name or other designation of the broker-dealer or other person from whom purchased or to whom sold?

If the bank has had an average of 200 or more securities transactions per year for customers over the prior three-calendar-year period, exclusive of transactions in U.S. government and federal agency obligations, answer questions 26, 27 and 28.

26. Does the bank maintain account records for each customer which reflect:
    a. All purchases and sales of securities?
    b. All receipts and deliveries of securities?
    c. All receipts and disbursements of cash for transactions in securities for such account?
    d. All other debits and credits pertaining to transactions in securities?
27. Does the bank maintain a separate memorandum (order ticket) of each order to purchase or sell securities (whether executed or cancelled) which includes:
    a. The account(s) for which the transaction was effected?
    b. Whether the transaction was a market order, limit order, or subject to special instructions?
    c. The time the order was received by the trader or other bank employee responsible for affecting the transaction?
    d. The time the order was placed with the broker-dealer, or if there was no broker-dealer, the time the order was executed or cancelled?
    e. The price at which the order was executed?

f. The broker-dealer used?

28. Does the bank maintain a record of all broker-dealers selected by the bank to effect securities transactions and the amount of commissions paid or allocated to each such broker during the calendar year?
29. Does the bank, subsequent to effecting a securities transaction for a customer, mail or otherwise furnish to such customer either a copy of the confirmation of a broker-dealer relating to the securities transaction or a written trade confirmation of a broker-dealer relating to the securities transaction or a written trade confirmation prepared by the bank?
30. If customer notification is provided by furnishing the customer with a copy of the confirmation of a broker-dealer relating to the transaction, and if the bank is to receive remuneration from the customer or any other source in connection with the transaction, and the remuneration is not determined pursuant to a written agreement between the bank and the customer, does the bank also provide a statement of the source and amount of any remuneration to be received?
31. If customer notification is provided by furnishing the customer with a trade confirmation prepared by the bank, does the confirmation disclose:
    a. The name of the bank?
    b. The name of the customer?
    c. Whether the bank is acting as agent for such customer, as principal for its own account, or in any other capacity?
    d. The date of execution and a statement that the time of execution will be furnished within a reasonable time upon written request of such customer?
    e. The identity, price and number of shares of units (or principal amount in the case of debt securities) of such securities purchased or sold by such customer?
32. For transactions which the bank effects in the capacity of agent, does the bank, in addition to the above, disclose:
    a. The amount of any remuneration received or to be received, directly or indirectly, by any broker-dealer from such customer in connection with the transaction?
    b. The amount of any remuneration received or to be received by the bank from the customer and the source and amount of any other remuneration to be received by the bank in connection with the transaction, unless remuneration is determined pursuant to a written agreement between the bank and the customer?
    c. The name of the broker-dealer used. Where there is no broker-dealer, the name of the person from whom the security was purchased or to whom it was sold, or the fact that such information will be furnished within a reasonable time upon written request?
33. Does the bank maintain the above records and evidence of proper notification for a period of at least three years?
34. Does the bank furnish the written notification described above within five business days from the date of the transaction, or if a broker-dealer is used, within five business days from the receipt by the bank of the broker-dealer's confirmation? If not, does the bank use one of the alternative procedures described in Regulation H?
35. Unless specifically exempted in Regulation H, does the bank have established written policies and procedures ensuring:
    a. That bank officers and employees who make investment recommendations or decisions for the accounts of customers, who particpate in the determination of such recommendations or decisions, or who, in connection with their duties, obtain information concerning which securities are being purchased or sold or recommended for such action, report to the bank, within 10 days after the end of the calendar quarter, all transactions in securities made by them or on their behalf, either at the bank or elsewhere in which they have a beneficial interest (subject to certain exemptions)?
    b. That in the above required report the bank officers and employees identify the securities purchased or sold and indicate the dates of the transactions and whether the transactions were purchases or sales?
    c. The assignment of responsibility for supervision of all officers or employees who (1) transmit orders to or place orders with broker-dealers, or (2) execute transactions in securities for customers?

d. The fair and equitable allocation of securities and prices to accounts when orders for the same security are received at approximately the same time and are placed for execution either individually or in combination?
e. Where applicable, and where permissible under local law, the crossing of buy and sell orders on a fair and equitable basis to the parties to the transaction?

OTHER

36. Are the preparation, additions, and posting of subsidiary records performed and/or adequately reviewed by persons who do not also have sole custody of securities?
37. Are subsidiary records reconciled, at least monthly, to the appropriate general ledger accounts and are reconciling items adequately investigated by persons who do not also have sole custody of securities?
38. Are fails to receive and deliver under a separate general ledger control?
    a. Are fail accounts periodically reconciled to the general ledger, and any differences followed up to a conclusion?
    b. Are periodic aging schedules prepared (if so, indicate frequency _____)?
    c. Are stale fail items confirmed and followed up to a conclusion?
    d. Are stale items valued periodically and, if any potential loss is indicated, is a particular effort made to clear such items or to protect the bank from loss by other means?
39. With respect to securities loaned and borrowed positions:
    a. Are details periodically reconciled to the general ledger, and any differences followed up to a conclusion?
    b. Are positions confirmed periodically (if so, indicate frequency _____)?
40. Is the compensation of all department employees limited to salary and a nondepartmentalized bonus or incentive plan?
    a. Are sales representatives' incentive programs based on sales volume and not department income?

CONCLUSION

41. 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.
42. Based on a composite evaluation, as evidenced by answers to the foregoing questions, internal control is considered (adequate/inadequate).

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

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.

on 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[19] 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).[20] 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[21] that offer or maintain one or more "covered accounts" must develop and implement a written Identity Theft Prevention Program (Program).[22] 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).

19. 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).

20. Section 111 of the FACT Act defines "identity theft" as "a fraud committed or attempted using the identifying information of another person."

21. 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.

22. "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,[23]

- 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

23. Examples of Red Flags from each of these categories are appended as supplement A to appendix J.

opening an account.[24] 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 com-

24. 31 U.S.C. 5318(l) (31 CFR 103.121).

plying with the rules and guidelines for outsourcing 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 secu-

rity 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.[25] 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

25 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.

handling funds or implementing credit decisions; 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.[26]
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.[27] 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 Stan-

26. 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.

27. 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.

dards No. 55." These statements contain the external-auditor reporting tools commonly used for service providers. SAS 70 reports, 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 organi-

zation 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.

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?

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 5300.1, "Information Technology," and the *FFIEC Information Systems Examination Handbook*.

10. See section 5300.1, "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.

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 responsibilities 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?

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.

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 Gov-*

erning 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 policy is a program to control the risks in the payment system, including institutions' use of

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.

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 institution that maintains an account at a Federal Reserve Bank is assigned or may establish a net

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.

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 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

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.

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 analy-

sis. 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 over-

drafts 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 an institution that requests additional daylight-overdraft capacity to decide on the appropriate max cap level. When considering the institu-

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.

tion'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.

Each institution that performs a self-assessment for a net debit cap should establish daylight-

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.

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 Bank may assign the institution a zero cap. In

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.

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.

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 equiva-

lency 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 amount of the cap that is not allocated to offices

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.

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 requirements and do not have regular access to

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 under the Federal Reserve's Regulation D (12 CFR 204) because it is organized solely to do business with other

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 evaluation of credit, liquidity, and operational risks.

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.

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.

Examination procedures are available on the Examination Documentation (ED) modules page on the Board's website. See the following ED module for examination procedures on this topic:

- Electronic Funds Transfer Risk Assessment