4000—MANAGEMENT ACTIVITIES AND INTERNAL CONTROLS

The 4000 series of sections explain key concepts related to bank management and internal controls. These sections address the supervisory approach for the assessment of a bank's risk management practices over certain banking activities. There are also sections on key aspects of an effective internal controls framework.

Directors are placed in a position of trust by the bank's shareholders, and both statutes and common law place responsibility for the affairs of a bank firmly and squarely on the board of directors. The board of directors of a bank should delegate the day-to-day routine of conducting the bank's business to its officers and employees, but the board cannot delegate its responsibility for the consequences of unsound or imprudent policies and practices, whether they involve lending, investing, protecting against internal fraud, or any other banking activity. The board of directors is responsible to the bank's depositors, other creditors, and shareholders for safeguarding their interests through the lawful, informed, efficient, and able administration of the institution. In the exercise of their duties, directors are governed by federal and state banking, securities, and antitrust statutes, as well as by common law, which imposes a liability on directors of all corporations. Directors who fail to discharge their duties completely or who are negligent in protecting the interests of depositors or shareholders may be subject to removal from office, criminal prosecution, civil money penalties imposed by bank regulators, and civil liability. See section 5040 of this manual, "Formal Corrective Actions," which describes those enforcement powers in greater detail.

DIRECTOR SELECTION

The affairs of each state member bank are overseen by its board of directors. The initial directors are elected by the shareholders at a meeting held before the bank is authorized to commence business. Thereafter, they are elected at meetings held at least annually on a day specified in the bank's bylaws. The directors hold office for a stated tenure, generally ranging from one to three years, or until their successors are elected and have qualified. No state member bank is to have less than five or more than 25 directors as specified in section 31 of the Banking Act of 1933. Various laws govern the election, number, qualifications, oath, liability, and removal of directors and officers, as well as the disclosure requirements for their outside business interests. Other laws pertain to certain restrictions, prohibitions, and penalties for securities dealers serving as directors, officers, or employees; director interlocks; purchases of assets from, or sales to, directors; commissions and gifts for procuring loans; embezzlement; abstraction; willful misapplication; false entries; political contributions; and other matters. The examiner must be familiar with these laws and the related regulations and interpretations.

DIRECTOR INDEPENDENCE

Directors must exercise their independent judgment when managing the bank's affairs. A responsible board will not merely rubber-stamp management's recommendations, but will review them carefully before deciding whether they are in the bank's best interests. A board that is excessively influenced by management, a single director, or a shareholder, or any combination thereof, may not be fulfilling its responsibilities to depositors, other creditors, and shareholders. Diversification of the board of directors is important and can be accomplished by including directors with no ownership or family-ownership interest in the bank and who are not employed by the bank.

A bank's board of directors may include one or more advisory directors. Advisory directors generally do not vote but may provide additional information or advice to the voting directors. An advisory director who functions in that capacity is generally not subject to the same regulatory requirements as voting members and has less liability for the board's actions. However, if an advisory director exercises a degree of influence or control over the board or the bank that is not commensurate with that status, it is appropriate for examiners to subject that individual to the same standards as voting directors. Such a person might also be subject to the same liability standards as a voting director.

DIRECTORS' RESPONSIBILITIES

Directors play a critical role in overseeing the affairs of the bank. Directors should understand that if they neglect to carry out their fiduciary duties and responsibilities, they may be financially liable if the bank fails or experiences loss. An examiner sometimes has to remind bank

directors of the extent of their duties and responsibilities. Unless bank directors realize the importance of their positions and act accordingly, they are failing to discharge their obligations to the shareholders, depositors, other creditors, and the community.

Selection of Competent Executive Officers

One of the board's most important duties is to select and appoint executive officers who are qualified to administer the bank's affairs effectively and soundly. The board is also responsible for removing officers who do not meet reasonable standards of honesty, competency, executive ability, and efficiency. The responsibility for selecting executive officers also entails retaining them and ensuring that competent successors can be promoted or hired to fill unanticipated voids. The board is responsible for evaluating the performance of the chief executive officer and approving the CEO's compensation. In many banks, the board also approves compensation for other executive officers.

A state member bank that has been chartered or undergone a change of control within the last two years, that is not in compliance with the minimum capital adequacy guidelines or regulations of the Board, or that is in an otherwise troubled condition must provide 30 days' written notice to its regulating Reserve Bank before it can add a director, promote an internal staff member to senior executive officer, or employ a new senior executive officer.

Effective Supervision of Bank Affairs

The type and degree of supervision required of a bank's board of directors to ensure a bank is soundly managed involve reasonable business judgment and competence and sufficient time to become informed about the bank's affairs. Directors ultimately are responsible for the soundness of the bank. If negligence is involved, a director may be personally liable. The responsibility of directors to supervise the bank's affairs may not be delegated to the active executive officers or anyone else. Directors may delegate to executive officers certain authority, but not the primary responsibility of ensuring that the bank is operated in a sound and legal manner.

Adoption and Adherence to Sound Policies and Objectives

The directors' role is to provide a clear framework of objectives and policies within which the chief executive officer can operate and administer the bank's affairs. This framework is often accomplished through the use of strategic plans and budgets. The strategic plan would discuss long-term, and in some cases, short-term goals and objectives as well as how progress toward their achievement will be measured. The objectives and policies should cover all areas of the bank's operations. The board of directors is responsible for establishing the policies that govern and guide the day-to-day operations of the bank, so they should review and approve them from time to time. These policies are primarily intended to ensure that the risks undertaken by the banks are prudent and are being properly managed. This means that the board of directors must, as a group, have a fundamental understanding of the various types of risks associated with different aspects of the banking business, for example, credit risk, foreign-exchange risk, or interest-rate risk, and define the types of risks the bank will undertake. Some of the more important areas in which policies and objectives must be established include investments, loans, asset and liability management, profit planning and budgeting, capital planning, and personnel. Directors are also responsible for adopting policies and procedures required by law or regulation, such as real estate lending policies, a security program, an interbank liabilities policy, and a Bank Secrecy Act program. The examination of these policies is covered in other sections of this manual.

Avoidance of Self-Serving Practices

A bank's directors bear a greater than normal responsibility for upholding safe and sound practices in dealing with transactions involving other members of the directorate and their related interests. Directors' decisions must preclude the possibility of partiality or favored treatment. Unwarranted loans to a bank's directors or their interests can be a serious safety-

and-soundness concern for the bank. Directors who become financially dependent on their bank normally lose their usefulness as directors. Other self-serving practices the examiner should watch for are—

- gratuities paid to directors to obtain their approval of financing arrangements or the use of particular services,
- the use of bank funds by directors, officers, or shareholders to obtain loans or transact other business (Directors should be especially critical of correspondent bank balances when officers, directors, or shareholders are borrowing from the depository bank. The Department of Justice's position is that certain interbank deposits connected with a loan to officers, directors, or shareholders of the depositing bank might constitute a misapplication of funds in violation of 18 USC 656), and
- transactions involving conflicts of interest (When board decisions involve a potential conflict of interest, the director with the potential conflict should fully disclose the nature of the conflict and abstain from voting on the matter. The abstention should be recorded in the minutes. The examiner should also be aware that ethical conflicts of interest can arise when a director or director-related firm performs professional services for the bank. For example, a director who is also the bank's legal counsel may not, in some situations, be able to advise or represent the bank objectively.).

Awareness of the Bank's Financial Condition and Management Policies

Management Information Systems

A management information system (MIS) provides the information, often originated from an institution's mainframe and microcomputers, necessary to manage an organization effectively. MIS should have clearly defined guidelines, policies, practices, standards, and procedures for the organization. These should be incorporated in the development, maintenance, and use of MIS throughout the institution.

MIS is used by all levels of bank staff to monitor various aspects of bank operations, up to and including its overall risk-management process. Therefore, MIS should be supportive of the institution's longer term strategic goals and objectives. At the other extreme, these everyday financial accounting systems also are used to ensure that basic control is maintained over financial recordkeeping activities. Since numerous decisions are based on MIS reports, appropriate control procedures must be set up to ensure that information is correct and relevant.

Audits

In May 1993, pursuant to requirements of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), the FDIC issued rules and guidelines that require all banks with total assets in excess of $500 million to have annual audits by an independent public accountant. Copies of these audit reports are to be sent to the FDIC and the appropriate Federal Reserve Bank. Furthermore, the Federal Reserve encourages banks with assets of $500 million or less to provide for annual audits by independent public accountants.

The board or a committee designated by the board should review the audit reports with the bank's management and the independent public accountants. The review should include—

- the scope of services required by the audit, significant accounting policies, and audit conclusions regarding significant accounting estimates;
- the adequacy of internal controls, and actions necessary to ensure the resolution of any problems or deficiencies; and
- the institution's compliance with applicable laws and regulations.

Many states have laws requiring directors' examinations of the bank. When the directors lack adequate knowledge of examination techniques and procedures, they are encouraged to employ a qualified accountant or other specialist to conduct all or part of this examination. The examining committee or the entire board should play an active role. Directors should obtain a clear understanding of the scope of the procedures to be employed, and the final report of the directors' examination should be reviewed by the board of directors.

Further guidance on the use of audit reports and the reliance placed upon the work of external and internal auditors in the examination

process can be found in the "Internal and External Audit Section" of this manual.

Maintenance of Reasonable Capitalization

A board of directors has the responsibility for maintaining its bank on a sufficiently capitalized basis. Capital planning and capital adequacy are discussed in the manual section "Assessment of Capital Adequacy," and the examiner should be familiar with this information.

Compliance with Banking Laws and Regulations

Directors must carefully observe that banking laws are not violated; they may be personally liable for losses arising out of illegal actions. In addition, civil money penalties can be assessed for unsafe and unsound actions that do not necessarily involve a violation of a banking law.

Guarantee of a Beneficial Influence on the Community's Economy

One reason for approving a newly chartered bank for Federal Reserve membership is to meet a specific community need. Directors, therefore, have a continuing responsibility to provide those banking services which meet the legitimate credit and other needs of the community being served. Directors should be certain that the bank attempts to satisfy all legitimate credit needs of the community.

BOARD MEETINGS

The board should conduct its business in meetings held as required by the bank's bylaws or state law. Regular meetings of the board should review statements showing the bank's financial condition and earnings; the investment portfolio; and loan activity, including past-due and nonaccrual loans, charged-off or recovered loans, large new loans, and loans to insiders. Directors should also review and approve all policies annually, and review and approve all insurance policies as they are obtained or renewed. They should also review audit and examination reports and initiate action to correct any deficiencies noted, review correspondence with regulatory agencies, review pending litigation, and keep informed of any major prospective undertakings, such as mergers, acquisitions, or new branches or construction.

Minutes of Board Meetings

The board should ensure that an accurate, adequate record of its actions is maintained. Such a record is usually kept in the form of minutes of the board meetings. The minutes should document the board's review of all regular items mentioned above as well as the review and discussion of all significant items that are not part of the regular meeting. Additionally, at a minimum, the minutes should record the attendance or absence of each director at each meeting, detail the establishment and composition of any committees, and note the abstention of any director from any vote. Examiners should review the minutes of board meetings, as well as a sample package prepared for a board meeting, to determine that directors are receiving adequate information to make informed, sound decisions. Meetings conducted by telephone, if allowable under state law, should be documented as thoroughly as regular meetings.

BOARD COMMITTEES

Many boards elect to delegate some of their workload to committees. The extent and nature of the bank's activities and the relative expertise of each board member play key roles in the board's determination of which committees to establish, who sits on them, and how much authority they have. Thus, there is no ideal committee structure. However, committees frequently found in state member banks include the following:

- *Executive Committee*—may be empowered to act when the full board is unable to meet, for example, between regular meetings. An executive committee is usually found in large institutions, where it relieves the full board of the burden of reviewing the details of financial statements and operational activities.

- *Audit Committee*—typically monitors compliance with bank policies and procedures, and reviews internal and external audit reports and bank examination reports. Because it is responsible for ensuring compliance, accuracy, and integrity throughout the organization, the audit committee should consist only of outside directors. The audit committee may supervise the bank's internal auditor and his or her staff directly by hiring personnel, evaluating their performance, and setting their compensation.
- *Loan Committee*—may be established to monitor underwriting standards and loan quality, and to ensure that lending policies and procedures are adequate. In most banks with loan committees, all new loans are reviewed by the loan committee either before or after funding, with the threshold for prior approval being the amount of either the loan or the aggregate debt to the borrower. The loan committee may also be responsible for the loan review function and for maintaining an adequate reserve for loan losses.
- *Investment or Asset-Liability Management Committee*—monitors the bank's investment policies, procedures, and holdings portfolio to ensure that goals for diversification, credit quality, profitability, liquidity, community investment, pledging requirements, and regulatory compliance are met. In some banks whose complexity warrants it, asset-liability management committees have been established to replace or supplement investment committees. An asset-liability management committee monitors the bank's balance sheet and external forces, notably interest rates, to help coordinate asset acquisition and funding sources.
- *Other Committees*—depending on the nature and complexity of the bank's business, the board may establish other committees to monitor such areas as trust, branching, new facilities construction, personnel/human resources, electronic data processing, and consumer compliance.

Minutes of all major actions taken by committees that play a significant role in managing the bank should be kept and meet the same minimum standards used for minutes of meetings of the full board.

COMPLIANCE WITH FORMAL AND INFORMAL SUPERVISORY ACTIONS

Bank directors must ensure that management corrects deficiencies found in the bank. Instructions to do so may come from the Federal Reserve as a formal or informal supervisory action, depending on the severity of the problem.

Formal actions, which include cease-and-desist orders and written agreements, are normally exercised when banks have serious problems. For less serious problems, the Federal Reserve issues informal actions such as a "memorandum of understanding." Informal actions are an agreement between the Reserve Bank and the bank that sets forth the required corrective actions. The Reserve Banks are generally responsible for monitoring compliance with both types of supervisory actions. To assist in that process, the Reserve Bank normally receives and evaluates periodic progress reports from the bank. In addition, information is provided by the examiner, who checks the bank's compliance with the action. The Reserve Banks may initiate additional supervisory action against the bank or individuals associated with it when compliance is insufficient.

Examiners should briefly discuss compliance with any enforcement actions on the Examination Conclusions and Comments page and direct the board of directors' attention to the Compliance with Enforcement Actions page of the examination report. The type and date of the action or resolutions and parties to the action should be listed. In addition, the examiner should generally list each provision requiring action by the bank and provide a comment addressing compliance with that provision. The examiner should comment on how the bank accomplished compliance or the problems that have prevented compliance. While certain information might be better discussed in the confidential section of the report, it is appropriate to make all salient negative comments on the Compliance with Enforcement Actions page to ensure that bank directors are notified of the remaining deficiencies that need to be corrected.

The Reserve Bank may recommend termination or modification of a formal supervisory action whenever it determines that the action has satisfactorily served its purpose and should be removed or modified. In these cases, the Reserve

Bank will send a memorandum with the appropriate explanation to the Board's Division of Supervision and Regulation (S&R) for review and evaluation. S&R and the Board's Legal Division, when appropriate, will prepare the documents necessary to terminate or modify the existing formal supervisory action.

Duties and Responsibilities of Directors

Examination Objectives

Effective date November 1995

Section 4000.2

1. To determine whether the board of directors fully understands its duties and responsibilities.

2. To determine if the board of directors is discharging its responsibilities in an appropriate manner.

3. To determine whether the board of directors has developed adequate objectives and policies.
4. To determine the existence of any conflicts of interest or self-dealing.
5. To determine compliance with laws and regulations.

1. Update the following and review for possible violations of law—
   a. A list of directors to include—
      - home address (If the director was appointed or elected since the previous examination, state the number of years residing at present address.),
      - date of birth,
      - years as a director of the bank,
      - approximate net worth,
      - occupation,
      - citizenship,
      - common stock ownership (beneficial, direct, and indirect), and
      - bonuses, fees, etc.

   b. A list of embezzlements, defalcations, misappropriations, mysterious disappearances, or thefts that have occurred since the last examination. That list should be signed by the chief executive officer or the auditor.
   c. A list of management officials (as defined in the Depository Institution Management Interlocks Act) of the bank, its holding company, and holding company affiliates who are management officials of other depository institutions.
   d. A list of the indebtedness of directors, executives officers, and principal shareholders to the bank examined and any other bank, along with a statement of the terms and conditions of each extension of credit.
2. Obtain or update a listing of all areas of the bank's operations that are administered under the provisions of written objectives and policies that have been developed by or with the approval of the board. Inform the examiners assigned to review those departments that a policy has been developed or an update has occurred.
3. Analyze the listing obtained in step 2, and note any area of banking activity for which policies should be developed.
4. Determine that the board has accepted its responsibility to effectively supervise the affairs of the bank and to be informed of the bank's condition by performing the following:
   a. Obtain a complete set of the latest reports furnished to directors at the last meeting, and list the areas of operation covered by the reports.
   b. Distribute copies of the reports to the examiners in other areas, and request that they determine if reports furnished to the board are prepared accurately, contain sufficient detail to allow the directors to make an intelligent decision, and are submitted on a timely basis.
   c. Prepare a list of areas not reporting or of reports the board does not receive that are considered necessary to maintain adequate supervision. As guidelines, consider the following reports:
      - A monthly statement of condition or balance sheet and a monthly statement of income. Those statements should be in reasonable detail and should be compared with the prior month, with the same month of a prior year, and with the budget. The directors should receive explanations for all large variances.
      - Monthly statements of changes in all capital and reserve accounts. Such statements should explain any changes.
      - Investment reports that group the securities by classifications; that reflect the book value, fair market value, and yield; and that include a summary of purchases and sales.
      - Loan reports that list significant past-due loans, trends in delinquencies, rate reductions, non-income-producing loans, and large new loans granted since the last report.
      - Audit and examination reports. Deficiencies in these reports should produce a prompt and efficient response from the board. The reports reviewed and actions taken should be reflected in minutes of the board of directors meetings.
      - A full report of all new executive-officer borrowing at any bank.
      - A monthly listing of type and amount of borrowing by the bank.
      - An annual presentation of bank insurance coverage.

- All correspondence addressed to the board of directors from the Federal Reserve and any other source.
- A monthly analysis of the bank's liquidity position.
- An annual projection of the bank's capital needs.
- A listing of any new litigation and a status report on existing litigation and potential exposure.
- A thorough report on any major bank endeavor that each bank director is expected to make a decision on, including branch applications and major building plans.

d. Determine the mechanism used to assign responsibility for correcting deficiencies noted in regulatory reports, internal audit reports, external audit reports, or any other reports to the board, and determine the board's system of determining compliance with such recommendations.
e. Determine how directors perform a director's examination, the frequency of such examinations, and what part the directors take in the process.
f. Review the bank's method of ensuring continued or resumed operations in the event of a disaster. Complete the emergency preparedness measures questionnaire for inclusion in the workpapers.
g. Review correspondence between the Federal Reserve and the bank to determine that it has been properly reported.

5. Determine evidence of conflicts of interest and self-dealing by—
   a. obtaining and summarizing information on the business interests of directors, executive officers, and principal shareholders;
   b. comparing that information to develop a list of directors who have business interests in common;
   c. analyzing the interests of directors to determine if the board consists of a variety of individuals;
   d. obtaining from the examiner assigned to assessment of capital adequacy a list of shareholders who own or control, either directly or indirectly, 5 percent or more of any class of voting security;
   e. distributing a list of the insiders (directors, officers, and shareholders whose ownership of voting securities in the institution is more than 10 percent) and their related interests to the appropriate examining personnel to ascertain the extent of loans to or transactions with insiders and their interests (Those examiners should be alert for any relationships with insiders' interests that are not included on the list.);
   f. requesting that the appropriate examiners determine if any transactions with insiders are on terms more favorable than those offered to other customers (If so, determine whether the board has approved such transactions.);
   g. determining that directors have reviewed their correspondent bank accounts in relation to possible conflicts of interest arising from directors', officers', or shareholders' borrowing from depository banks; and
   h. correlating all information on insider transactions, and preparing appropriate report comments.
6. Obtain the minutes of the meetings of the board of directors, the charter, the bylaws, and the minutes of shareholders meetings.
   a. Review and summarize the bylaws and charter of the organization, including any specific provisions on the requirements of directors. The resulting material should become a permanent part of the workpapers and should be updated at subsequent examinations.
   b. Read and summarize the minutes of all meetings of the board since the last examination, making certain to—
      - list any actions taken in contravention of the bylaws;
      - record major actions taken by the board that are not a part of a normal monthly meeting;
      - record any resolution or discussion covering the development of or entrance into a new area, such as a geographic area, customer service, asset category, or liability category;
      - record the creation of any special committee and the area with which it is designed to deal;
      - determine that actions taken by standing committees are reviewed and ratified by the full board;
      - if the minutes specify any transactions with directors or their interests, deter-

mine that the abstention of any interested director from voting on the matters is noted;
- if the minutes do not mention any director-related transactions that have been uncovered during the examination, inquire if the interested director did refrain from voting.

c. Read and summarize the minutes of the board's annual organization meeting and—
- list standing committees and their members,
- have examiners who are examining areas that have standing-committee supervision read and summarize the minutes of those committees, and
- prepare a list of major areas of operation that are not monitored by specific committees.

d. Read and summarize the minutes of any stockholders meetings. The summary should include a list of directors elected at the annual meeting, the number of shares present and voted, individuals acting as proxies, and specific action approved by shareholders.

e. Ascertain during the review of shareholders meeting minutes that (1) shareholders' approval has been received; (2) the bank's charter has been amended, if necessary; and (3) compliance with appropriate state or federal statutes has been met for the following:
- any establishment of or change of a branch location
- any issuance of preferred stock
- any increase in capital stock, either through sale or a stock dividend
- any reduction in capital stock (and ascertain whether the resultant capital is not below what is required by the capital adequacy guidelines)
- any stock split
- any bank pension plan established since the preceding examination
- any bank involvement in a conversion, merger, or consolidation
- all other matters subject to vote

f. Determine the date of the annual shareholders meeting and if it was in compliance with the bylaws.

g. Review the charter and/or bylaws for quorum requirements of shareholder meetings. Ascertain that, at any meeting, the quorum requirements were satisfied according to recorded requirements or by having more than one-half of the eligible shareholders represented.

h. Review any stock option or stock purchase plan adopted since the preceding examination, and review such action for compliance with the various conditions involving charter and shareholder approval.

i. Determine if any candidate was nominated for director, other than the slate nominated by bank management, and review for compliance with the appropriate state statute.

7. Determine that the directors have accepted their responsibility for selecting competent officers by—
   a. determining that the board or a committee thereof reviews, at least annually, the chief executive officer's performance in attaining or progressing toward attaining specific objectives or goals set by the board,
   b. determining if a policy statement on personnel exists, and ascertaining what provisions the board has made for successor management,
   c. determining if any management contracts exist and, if one does, obtaining a copy, summarizing the pertinent points, and determining the reasonableness of terms,
   d. determining by inquiry how the remuneration of executive officers is set and who makes decisions concerning executive salaries, and
   e. listing any titled individual who, by action of the board, is specifically excluded from being an executive officer.
8. Determine compliance with laws and regulations by—
   a. reviewing workpapers of other examination areas or discussing compliance with other examiners to determine any violations of laws or regulations concerning directors that were disclosed in these examination areas,
   b. reviewing the nature and extent of violations discovered at prior examinations to determine if similar violations have occurred at this examination, and
   c. correlating information obtained from the minutes of board meetings to the reports of officer borrowings that have

been prepared at and forwarded from other banks to determine that all such borrowings have been reported to the board.

9. Determine compliance with the Foreign Corrupt Practices Act (15 USC 78dd-1 and -2) by—
   a. reviewing the bank's policy prohibiting improper or illegal payments, bribes, kickbacks, etc., to any foreign government official or other person or organization covered by the law;
   b. determining how that policy has been communicated to officers, employees, or agents of the bank;
   c. reviewing any investigation or study done by, or on behalf of, the board of directors on the bank's policies and operations concerning the advance of funds in possible violation of the act;
   d. reviewing the work done by the examiner assigned to internal control to determine whether internal or external auditors have established routines to discover improper or illegal payments;
   e. analyzing the general level of internal control to determine whether there is sufficient protection against the inaccurate recording of improper or illegal payments on the bank's books;
   f. requesting that examiners working in other areas of the bank be alert for any transactions that might violate the provisions of the act;
   g. compiling any information discovered throughout the examination on possible violations; and
   h. performing procedures on suspected criminal violations as outlined in section 5020.3, "Overall Conclusions Regarding Condition of the Bank: Examination Procedures."
10. Answer the following questions. (This questionnaire is intended to be a quick review for determining that all laws and regulations pertaining to directors have been complied with. Questions should be answered "no" and sub-questions should be answered "yes." Any deviation from this pattern indicates a violation or potential violation. Situations that are not judged to be violations require comments stating the basis for that judgment.)
    a. Is the number of directors less than 5 or greater than 25 (section 31, Banking Act of June 16, 1933)?
    b. Have any directors failed to qualify by reason of insufficient stock ownership (12 USC 72)?
    c. Are any directors noncitizens of the United States (12 USC 72)? If so, has the citizenship requirement been waived?
    d. Do more than one-third of the directors fail to reside in the state, territory, or district in which the bank is located, or within 100 miles of the bank's head office (12 USC 72)?
    e. Did more than one-third of the directors fail to reside in the state, territory or district in which the bank is located, or within 100 miles of the bank's head office, for one year before election (12 USC 72)?
    f. Are any transactions with directors or their related interests on more favorable terms than those offered to other customers (Regulation O (12 CFR 215))?
    g. Do the deposit accounts of directors receive greater interest than those of other customers (section 22(e), Federal Reserve Act (12 USC 376))?
    h. Have any provisions of a cease-and-desist agreement or order been violated (Rules of Practice for Hearings (12 CFR 263))?
    i. Has any director, officer, or employee been convicted of a crime involving a breach of trust or act of dishonesty (section 8(g) of the Federal Deposit Insurance Act (12 USC 1829))? If so, has the FDIC approved his or her membership on the board or employment?
    j. Have any tie-ins of services been authorized by the board (Regulation Y (12 CFR 225.7))?
    k. Were any loans to bank examiners disclosed (Criminal Code—18 USC 212 and 213)?
    l. Has the bank made any political contributions (Federal Election Campaign Act (12 USC 441b))?
    m. Have any employees been found to have misappropriated funds, made false entries, or otherwise defrauded the bank (18 USC 656)?
    n. Has an officer of the bank failed to make appropriate written reports when an

embezzlement, misapplication, or similar transaction occurred (SR-579)?

o. Have any extortionate extensions of credit been discovered (18 USC 892–894)?

p. Have any checks been certified against uncollected funds (18 USC 1004)?

q. Have unauthorized obligations of the bank been issued (18 USC 1005 and 1006)?

r. Has there been a change in control (Regulation Y (12 CFR 225.41–225.43))? If so, was the Federal Reserve notified and was the application approved?

s. Have any purchase-money loans been made that are secured by 25 percent or more of the stock of another secured bank (Regulation Y (12 CFR 225.41))? If so, have the appropriate authorities been notified?

t. Has the bank failed to maintain records of directors, executive officers, and principal shareholders and their related interests (Regulation O (12 CFR 215.8))?

u. Are management officials of the bank, or its holding company or holding company affiliates, also management officials of an unaffiliated depository institution or depository holding company (Regulation L (12 CFR 212))? If so—
   - was such relationship established prior to November 10, 1978, and previously permitted by section 8, Clayton Anti-Trust Act (15 USC 19)?
   - was prior approval of the Federal Reserve obtained for a relationship that was developed since November 10, 1978?
   - does the interlocking relationship meet the criteria of one of the exceptions permitted by Regulation L (12 CFR 212)?
   - is the management relationship with an institution whose—
     — principal offices or branches, excluding electronic terminals, are located in a different RMSA from the bank's or its holding company's offices or branches (does not apply if either institution has assets of less than $20 million) (12 CFR 212.3(b))?
     — principal offices or branches, excluding electronic terminals, are located in another city, town, or village not contiguous or adjacent and 10 miles or more apart?
   - if the bank or its holding company has assets exceeding $2.5 billion, does the interlocking management relationship exist with a nonaffiliated depository institution holding company with assets of $1.5 billion or less?

v. Have any loans to executive officers been uncovered that were not reported to the board (Regulation O (12 CFR 215) and 12 USC 503)?

w. Has a majority of the board failed to preapprove extensions of credit to any of the bank's executive officers, directors, or principal shareholders and their related interests when the total loans to the individual exceed the amount prescribed in Regulation O?

x. Has the bank notified executive officers and principal shareholders of their reporting requirements (Regulation O (12 CFR 215))?

11. Determine compliance with administrative actions by—
    a. reviewing provisions of the document and
    b. reviewing bank records and performing necessary procedures to isolate noncompliance.

12. Evaluate the bank's compliance with formal or informal administrative actions and prepare comments for page one of the examination report (SR-02-17 and SR-92-21). (See also section 5040.1.)

13. Determine compliance with conditions imposed in the approvals of corporate filings for—
    a. branches and relocation applications, including—
       - capital plans or capital injections,
       - fixed-asset limitations, and
       - CRA plans;
    b. subordinated debt, operating subsidiaries, and interim bank applications, including—
       - capital plans and
       - prior review and appropriate clearance of disclosures.

14. On the basis of the information obtained by performing the foregoing procedures, or any other procedures deemed appropriate, evaluate the adequacy and effectiveness of the board of directors. The evaluation should include, but is not limited to—

a. the frequency and effectiveness of meetings;
b. the effectiveness of board committees;
c. the directors' role in establishing policy;
d. the adequacy of the policies and major inconsistencies therein;
e. the quality of reports for directors, noting any deficiencies in information flows from operating management;
f. violations of laws and regulations;
g. whether any one person or group appears to control or dominate the board (if so, comment on any adverse effects on operating policies, procedures, or the overall financial condition of the bank); and
h. the board's responsiveness to recommendations from the auditors and supervisory authorities.

15. Update the workpapers with any information that will facilitate future examinations.

As part of their executive compensation and retention programs, banks and other financial institutions (collectively referred to in this section as ''institutions'') often enter into deferred compensation agreements with selected employees. These agreements are generally structured as nonqualified retirement plans for federal income tax purposes and are based on individual agreements with selected employees.

Institutions often purchase bank-owned life insurance (BOLI) in connection with many of their deferred compensation agreements. (See sections 4042.1 and 2210.1 for an explanation of the accounting for BOLI transactions). BOLI may produce attractive tax-equivalent yields that offset some or all of the costs of the agreements.

Deferred compensation agreements are commonly referred to as *indexed retirement plans* (IRPs) or as *revenue-neutral plans.* The institution's designated management and accounting staff that is responsible for the institution's financial reporting must regularly review the accounting for deferred compensation agreements to ensure that the obligations under the agreements are appropriately measured and reported in accordance with generally accepted accounting principles (GAAP). In so doing, the management and accounting staff should apply and follow Accounting Principles Board Opinion No. 12, ''Omnibus Opinion—1967,'' as amended by Statement of Financial Accounting Standards No. 106 (FAS 106), ''Employers' Accounting for Postretirement Benefits Other Than Pensions'' (hereafter referred to as APB 12).

IRPs are one type of deferred compensation agreement that institutions enter into with selected employees. IRPs are typically designed so that the spread each year, if any, between the tax-equivalent earnings on the BOLI covering an individual employee and a hypothetical earnings calculation is deferred and paid to the employee as a post-retirement benefit. This spread is commonly referred to as *excess earnings.* The hypothetical earnings are computed on the basis of a predefined variable index rate (for example, the cost of funds or the federal funds rate) times a notional amount. The notional amount is typically the amount the institution initially invested to purchase the BOLI plus subsequent after-tax benefit payments actually made to the employee. By including the after-tax benefit payments and the amount initially invested to purchase the BOLI in the notional amount, the hypothetical earnings reflect an estimate of what the institution could have earned if it had not invested in the BOLI or entered into the IRP with the employee. Each employee's IRP may have a different notional amount on which the index is based. The individual IRP agreements also specify the retirement age and vesting provisions, which can vary from employee to employee.

An IRP agreement typically requires the excess earnings that accrue before an employee's retirement to be recorded in a separate liability account. Once the employee retires, the balance in the liability account is generally paid to the employee in equal, annual installments over a set number of years (for example, 10 or 15 years). These payments are commonly referred to as the *primary benefit* or *pre-retirement benefit.*

An employee may also receive the excess earnings that are earned after his or her retirement. This benefit may continue until the employee's death and is commonly referred to as the *secondary benefit* or *post-retirement benefit.* The secondary benefit is paid annually, once the employee has retired, and is in addition to the primary benefit.

Examiners should be aware that some institutions may not be correctly accounting for the obligations under an IRP. Because many institutions were incorrectly accounting for IRPs, the federal banking and thrift agencies issued on February 11, 2004, an Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance. (See SR-04-4.) The guidance is stated here, except for the information on the reporting of deferred compensation agreement obligations in the bank Call Reports and on changes in accounting for those agreements. Examiners should determine whether an institution's deferred compensation agreements are correctly accounted for. If the accounting is incorrect, assurance should be obtained from the institution's management that corrections will be made in accordance with GAAP and the advisory's instructions for changes in accounting. The examiner's findings should be reported in the examination report. Also report the nature of the accounting errors and the estimated financial impact that correcting the errors will have on the institution's

financial statements, including its earnings and capital position.

ACCOUNTING FOR DEFERRED COMPENSATION AGREEMENTS, INCLUDING IRPs

Deferred compensation agreements with select employees under individual contracts generally do not constitute post-retirement income plans (that is, pension plans) or post-retirement health and welfare benefit plans. The accounting for individual contracts that, when taken together, do not represent a post-retirement plan should follow APB 12. If the individual contracts, taken together, are equivalent to a plan, the plan should be accounted for under Statement of Financial Accounting Standards No. 87, "Employers' Accounting for Pensions," or under FAS 106.

APB 12 requires that an employer's obligation under a deferred compensation agreement be accrued according to the terms of the individual contract over the required service period to the date the employee is fully eligible to receive the benefits, or the *full eligibility date.* Depending on the individual contract, the full eligibility date may be the employee's expected retirement date, the date the employee entered into the contract, or a date between these two dates. APB 12 does not prescribe a specific accrual method for the benefits under deferred compensation contracts, stating only that the "cost of those benefits shall be accrued over that period of the employee's service in a systematic and rational manner." The amounts to be accrued each period should result in a deferred compensation liability at the full eligibility date that equals the then-present value of the estimated benefit payments to be made under the individual contract.

APB 12 does not specify how to select the discount rate to measure the present value of the estimated benefit payments. Therefore, other relevant accounting literature must be considered in determining an appropriate discount rate. An institution's incremental borrowing rate[1] and the current rate of return on high-quality fixed-income debt securities[2] should be the acceptable discount rates to measure deferred compensation agreement obligations. An institution must select and consistently apply a discount-rate policy that conforms with GAAP.

For each IRP, an institution should calculate the present value of the expected future benefit payments under the IRP at the employee's full eligibility date. The expected future benefit payments can be reasonably estimated. They should be based on reasonable and supportable assumptions and should include both the primary benefit and, if the employee is entitled to excess earnings that are earned after retirement, the secondary benefit. The estimated amount of these benefit payments should be discounted because the benefits will be paid in periodic installments after the employee retires. The number of periods the primary and any secondary benefit payments should be discounted may differ because the discount period for each type of benefit payment should be based on the length of time during which each type of benefit will be paid, as specified in the IRP.

After the present value of the expected future benefit payments has been determined, the institution should accrue an amount of compensation expense and a liability each year from the date the employee enters into the IRP until the full eligibility date. The amount of these annual accruals should be sufficient to ensure that a deferred compensation liability equal to the present value of the expected benefit payments is recorded by the full eligibility date. *Any method of deferred compensation accounting that does not recognize some expense for the primary benefit and any secondary benefit in each year from the date the employee enters into the IRP until the full eligibility date is not considered to be systematic and rational.*

Vesting provisions should be reviewed to ensure that the full eligibility date is properly determined because this date is critical to the measurement of the liability estimate. Because APB 12 requires that the present value of the expected benefit payments be recorded by the full eligibility date, institutions also need to consider changes in market interest rates to appropriately measure deferred compensation

1. Accounting Principles Board Opinion No. 21, "Interest on Receivables and Payables," paragraph 13, states in part that "the rate used for valuation purposes will normally be at least equal to the rate at which the debtor can obtain financing of a similar nature from other sources at the date of the transaction."

2. FAS 106, paragraph 186, states that "[t]he objective of selecting assumed discount rates is to measure the single amount that, if invested at the measurement date in a portfolio of high-quality debt instruments, would provide the necessary future cash flows to pay the accumulated benefits when due."

liabilities. Therefore, to comply with APB 12, institutions should periodically review both their estimates of the expected future benefits under IRPs and the discount rates used to compute the present value of the expected benefit payments, and revise those estimates and rates, when appropriate.

Deferred compensation agreements, including IRPs, may include noncompete provisions or provisions requiring employees to perform consulting services during post-retirement years. If the value of the noncompete provisions cannot be reasonably and reliably estimated, no value should be assigned to the noncompete provisions in recognizing the deferred compensation liability. Institutions should allocate a portion of the future benefit payments to consulting services to be performed in post-retirement years only if the consulting services are determined to be substantive. Factors to consider in determining whether post-retirement consulting services are substantive include but are not limited to (1) whether the services are required to be performed, (2) whether there is an economic benefit to the institution, and (3) whether the employee forfeits the benefits under the agreement for failure to perform such services.

APPENDIX—EXAMPLES OF ACCOUNTING FOR DEFERRED COMPENSATION AGREEMENTS

The following are examples of the full-eligibility-date accounting requirements for a basic deferred compensation agreement. The assumptions used in these examples are for illustrative purposes only. An institution must consider the terms of its specific agreements, the current interest-rate environment, and current mortality tables in determining appropriate assumptions to use in measuring and recognizing the present value of the benefits payable under its deferred compensation agreements.

Institutions that enter into deferred compensation agreements with employees, particularly more-complex agreements (such as IRPs), should consult with their external auditors and their respective Federal Reserve Bank to determine the appropriate accounting for their specific agreements.

Example 1: Fully Eligible at Agreement Inception

A company enters into a deferred compensation agreement with a 55-year-old employee who has worked five years for the company. The agreement states that, in exchange for the employee's past and future services and for his or her service as a consultant for two years after retirement, the company will pay an annual benefit of $20,000 to the employee, commencing on the first anniversary of the employee's retirement. The employee is fully eligible for the deferred compensation benefit payments at the inception of the agreement, and the consulting services are not substantive.

Other key facts and assumptions used in determining the benefits payable under the agreement and in determining the liability and expense the company should record in each period are summarized in the following table:

Expected retirement age	60
Number of years to expected retirement age	5
Discount rate (%)	6.75
Expected mortality age based on present age	70

At the employee's expected retirement date, the present value of a lifetime annuity of $20,000 that begins on that date is $142,109 (computed as $20,000 times 7.10545, the factor for the present value of 10 annual payments at 6.75 percent). At the inception date of the agreement, the present value of that annuity of $102,514 (computed as $142,109 times 0.721375, the factor for the present value of a single payment in five years at 6.75 percent) is recognized as compensation expense because the employee is fully eligible for the deferred compensation benefit at that date.

The following table summarizes *one* systematic and rational method of recognizing the expense and liability under the deferred compensation agreement:

Year	A *Benefit payment ($)*	B *Service component ($)*	C *Interest component ($)*	D (B + C) *Compensation expense ($)*	E *Beginning-of-year liability ($)*	F (E + D – A) *End-of-year liability ($)*
0	–	102,514	–	102,514	–	102,514
1	–	–	6,920	6,920	102,514	109,434
2	–	–	7,387	7,387	109,434	116,821
3	–	–	7,885	7,885	116,821	124,706
4	–	–	8,418	8,418	124,706	133,124
5	–	–	8,985	8,985	133,124	142,109
6	20,000	–	9,593	9,593	142,109	131,702
7	20,000	–	8,890	8,890	131,702	120,592
8	20,000	–	8,140	8,140	120,592	108,732
9	20,000	–	7,339	7,339	108,732	96,071
10	20,000	–	6,485	6,485	96,071	82,556
11	20,000	–	5,572	5,572	82,556	68,128
12	20,000	–	4,599	4,599	68,128	52,727
13	20,000	–	3,559	3,559	52,727	36,286
14	20,000	–	2,449	2,449	36,286	18,735
15	20,000	–	1,265	1,265	18,735	0
Totals	200,000	102,514	97,486	200,000		

The following entry would be made at the inception date of the agreement (the final day of year 0) to record the service component of the compensation expense and related deferred compensation agreement liability:

	Debit	*Credit*
Compensation expense	$102,514	
Deferred compensation liability		$102,514

[To record the column B service component]

In each period after the inception date of the agreement, the company would adjust the deferred compensation liability for the interest component and any benefit payment. In addition, the company would reassess the assumptions used in determining the expected future benefits under the agreement and the discount rate used to compute the present value of the expected benefits in each period after the inception of the agreement, and revise the assumptions and rate, as appropriate.

Assuming that no changes were necessary to the assumptions used to determine the expected future benefits under the agreement or to the discount rate used to compute the present value of the expected benefits, the following entry would be made in year 1 to record the interest component of the compensation expense:

	Debit	*Credit*
Compensation expense	$6,920	
Deferred compensation liability		$6,920

[To record the column C interest component (computed by multiplying the prior-year column F balance by the discount rate)]

Similar entries (but for different amounts) would be made in year 2 through year 15 to record the interest component of the compensation expense.

The following entry would be made in year 6 to record the payment of the annual benefit:

	Debit	*Credit*
Deferred compensation liability	$20,000	
Cash		$20,000

[To record the column A benefit payment]

Similar entries would be made in year 7 through year 15 to record the payment of the annual benefit.

Example 2: Fully Eligible at Retirement Date

If the terms of the contract described in example 1 had stated that the employee is only entitled to receive the deferred compensation benefit if the sum of the employee's age and years of service equals 70 or more at the date of retirement, the employee would be fully eligible for the deferred compensation benefit at age 60, after rendering five more years of service. At the employee's expected retirement date, the present value of a lifetime annuity of $20,000 that begins on the first anniversary of that date is $142,109 (computed as $20,000 times 7.10545, the factor for the present value of 10 annual payments at 6.75 percent). The company would accrue this amount in a systematic and rational manner over the five-year period from the date it entered into the agreement to the date the employee is fully eligible for the deferred compensation benefit. Under *one* systematic and rational method, the annual service component accrual would be $24,835 (computed as $142,109 divided by 5.72213, the factor for the future value of five annual payments at 6.75 percent).

Other key facts and assumptions used in determining the benefits payable under the agreement and in determining the liability and expense the company should record in each period are summarized in the following table:

Expected retirement age	60
Number of years to expected retirement age	5
Discount rate (%)	6.75
Expected mortality age based on present age	70

The following table summarizes *one* systematic and rational method of recognizing the expense and liability under the deferred compensation agreement:

Year	A *Benefit payment ($)*	B *Service component ($)*	C *Interest component ($)*	D (B + C) *Compensation expense ($)*	E *Beginning-of-year liability ($)*	F (E + D – A) *End-of-year liability ($)*
1	–	24,835	–	24,835	–	24,835
2	–	24,835	1,676	26,511	24,835	51,346
3	–	24,835	3,466	28,301	51,346	79,647
4	–	24,835	5,376	30,211	79,647	109,858
5	–	24,835	7,416	32,251	109,858	142,109
6	20,000	–	9,593	9,593	142,109	131,702
7	20,000	–	8,890	8,890	131,702	120,592
8	20,000	–	8,140	8,140	120,592	108,732
9	20,000	–	7,339	7,339	108,732	96,071
10	20,000	–	6,485	6,485	96,071	82,556
11	20,000	–	5,572	5,572	82,556	68,128
12	20,000	–	4,599	4,599	68,128	52,727
13	20,000	–	3,559	3,559	52,727	36,286
14	20,000	–	2,449	2,449	36,286	18,735
15	20,000	–	1,265	1,265	18,735	0
Totals	200,000	124,175	75,825	200,000		

No entry would be made at the inception date of the agreement. The following entry would be made in year 1 to record the service component of the compensation expense and related deferred compensation agreement liability:

	Debit	*Credit*
Compensation expense	$24,835	
Deferred compensation liability		$24,835

[To record the column B service component]

Similar entries would be made in year 2 through year 5 to record the service component of the compensation expense.

In each subsequent period, until the date the employee is fully eligible for the deferred compensation benefit, the company would adjust the deferred compensation liability for the total expense (the service and interest components). In each period after the full eligibility date, the company would adjust the deferred compensation liability for the interest component and any benefit payment. In addition, the company would reassess the assumptions used in determining the expected future benefits under the agreement and the discount rate used to compute the present value of the expected benefits in each period after the inception of the agreement, and revise the assumptions and rate, as appropriate.

Assuming no changes were necessary to the assumptions used to determine the expected future benefits under the agreement or to the discount rate used to compute the present value of the expected benefits, the following entry would be made in year 2 to record the interest component of the compensation expense:

	Debit	*Credit*
Compensation expense	$1,676	
Deferred compensation liability		$1,676

[To record the column C interest component (computed by multiplying the prior-year column F balance by the discount rate)]

Similar entries (but for different amounts) would be made in year 3 through year 15 to record the interest component of the compensation expense.

The following entry would be made in year 6 to record the payment of the annual benefit:

	Debit	*Credit*
Deferred compensation liability	$20,000	
Cash		$20,000

[To record the column A benefit payment]

Similar entries would be made in year 7 through year 15 to record the payment of the annual benefit.

Sound Incentive Compensation Policies

Effective date October 2010

Section 4008.1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

SCOPE OF APPLICATION

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

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

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

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

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

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

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

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

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

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

PRINCIPLES OF A SOUND INCENTIVE COMPENSATION SYSTEM

Principle 1: Balanced Risk-Taking Incentives

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. Performance targets may have a material effect on risk-taking incentives. Such targets may offer employees greater rewards for increments of performance that are above

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

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

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

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

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

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

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

the target or may provide that awards will be granted only if a target is met or exceeded. Employees may be particularly motivated to take imprudent risk in order to reach performance targets that are aggressive but potentially achievable.

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

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

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

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

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

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

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

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

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

arrangement entered into by the organization do not encourage imprudent risk-taking in light of the other features of the employee's incentive compensation arrangements.

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

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

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

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

Principle 2: Compatibility with Effective Controls and Risk-Management

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

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

Such actions may significantly weaken the effectiveness of an organization's incentive compensation arrangements in restricting imprudent risk-taking. These actions can have a particularly damaging effect on the safety and soundness of the organization if they result in the weakening of risk measures, information, or judgments that the organization uses for other risk-management, internal control, or financial purposes. In such cases, the employee's actions

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

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

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

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

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

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

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

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

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

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

Other functions within an organization, such as its control, human resources, or finance func-

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

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

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

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

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

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

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

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

Principle 3: Strong Corporate Governance

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CONCLUSION ON SOUND INCENTIVE COMPENSATION

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

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

The purpose of this section is to guide the examiner in evaluating bank management. Although the directorate is an integral part of the overall management of a bank, the management appraisal examination program is concerned primarily with the active officers. A review of the quality of director guidance and supervision is covered in "Duties and Responsibilities of Directors."

It is the responsibility of directors to employ a competent chief executive officer. Thereafter, senior management normally assumes the responsibility to employ, maintain and educate a qualified staff. Since a direct relationship exists between the overall condition of a bank and the quality of management, the first priority in evaluating the condition of the bank is to make an accurate appraisal of the competency of the management team.

Management is responsible, not only for the operations of the bank and the quality of its assets on a day-to-day basis, but also for planning for the future. Senior management should be evaluated on its plans for maintaining or improving the condition of the bank in the future as well as on the bank's present condition. The depth of planning and a general forward looking attitude of executive officers should be considered when projecting future management impact. This should include an evaluation of management's efforts to provide for succession of senior bank officials.

The projection of future management impact involves an appraisal of the quality and quantity of senior and middle management. This assessment of course must be relative to the size and community circumstances of the bank. Examiners must not restrict their appraisals to the past and present. The past and present certainly are significant, requiring an in-depth analysis of financial condition, earnings and capital adequacy, both on an absolute basis and as a trend, but, the determination of what the management will do for the bank in the future is most significant. The System's goal is to prevent problems from developing rather than waiting for future examinations to identify deteriorating conditions.

Bank management receives strong pressure from customers, stockholders and competitors. Customers demand more for their money, in the form of both interest and services, and stockholders demand higher returns on their investments, both in dividends and increased market value of their stock. No bank is completely free from the pressure of competition and, for most institutions, this is one of the strongest forces felt. In the midst of those pressures, the clear mandate to bank management is to "perform." Performance is measured in terms of long-run profitability, liquidity and solvency. It is almost impossible for a bank to achieve those long-range goals unless careful planning and coordination bring efficiency to its activities. Management must recognize the bank's position in the market and make plans which will achieve the objectives set for the institution by the directors. It must be constantly alert to the need for continually upgrading and expanding services and facilities to support and encourage the bank's growth.

Both the directors and senior management have important roles in a bank's program of internal control and internal audit. Although directors have overall audit responsibility and should require that the auditor report directly to them, senior management normally is charged with the duty of maintaining a strong system of internal control.

The entire examination procedure, as outlined throughout this manual, is designed to provide a clear picture of both the present and anticipated future condition of the bank under examination. As a result, the reports and workpapers generated by the examination process will serve as a major tool for examiners in their evaluation of management. Examination procedures for various balance sheet accounts and departmental areas are designed to effect a comprehensive evaluation of internal control and internal and/or external audit, and will provide the examiner with insight into the degree of compliance with the bank's own written policies in such areas. Similarly, the examination procedures in "Loan Portfolio Management," "Investment Securities," "Funds Management," "Assessment of Capital Adequacy," and "Analytical Review and Income and Expense" are designed to lead to a detailed analysis of written objectives, policies and procedures in those management areas.

The examiner must take a practical approach to evaluating these features depending on the bank's characteristics. The examiner can have greater confidence in the continuity of top and middle management when it is known that the bank has an inflow of new personnel at various

levels and that training procedures and advancement policies will keep the organization viable and dynamic.

The examiner must be concerned with salary levels within the bank and must review information collected during the examination about the bank's employee benefits program. Salaries paid and benefits provided should be compared with those offered by an appropriate peer group, and inquiry should be made to determine the relationship between the bank's payroll structure and that offered by competitors for the same caliber personnel.

The examiner must judge the appropriateness of asset distribution in view of the bank's sources of funds. The examiner must evaluate the adequacy of the bank's capital position and expectations in view of asset quality and plans for growth and expansion. The overall management evaluation should be made by the examiner-in-charge, because he or she is in the best position to identify weaknesses and inconsistencies in policies. Although examiners-in-charge will rely heavily upon the information received from assisting examining personnel in various areas under review, it is their task to assemble all of such information into a composite picture of the quality of management.

Senior management is responsible for the quality of all bank personnel and for planning its own replacement. A bank's recruiting, training, and personnel development activities are vital to the development and continuity of a quality staff. The examiner must evaluate those areas to determine the quality of overall management. Some features of good personnel management are:

- An organizational structure.
- Detailed position descriptions.
- Carefully planned recruiting.
- Appropriate training.
- Performance review.
- Salary administration.
- Provision for communication.

The examiner should identify and interpret trends that can reveal flaws in policy either as written or as practiced. The examiner should question the quality of management in any area in which he or she finds serious shortcomings or makes significant criticisms.

The examiner should be alert for situations in which top management dominates the board or where top management acts solely at the direction of either the board or a dominant influence on the board. Although it is extremely important for the directors to assume their appropriate role in setting objectives and formulating policy consistent with their responsibilities to the depositors, shareholders and regulators, dialogue with top management must occur. In banks where both directors and senior management recognize and assume their appropriate duties and responsibilities, areas for conflict are greatly reduced.

1. To determine the consistency of written objectives, policies, and procedures in the various asset, liability, and operational areas.
2. To determine that policies are being adhered to throughout the system.
3. To determine that management plans adequately for future conditions and developments.
4. To evaluate the adequacy of the bank's personnel practices as they relate to management continuity.
5. To evaluate management experience and depth.
6. To determine that management has established systems which facilitate efficient operation and communication.
7. To evaluate the propriety and soundness of management decisions.
8. To project the impact of management on the future condition of the bank.

In the following procedural steps examiners should attempt to utilize already developed material from internal or external audit sources. Also, the examining resources and circumstances of the bank must be weighed in perspective to set the depth of scope for this area.

1. Obtain the following, if available:
   a. Organization chart.
   b. Management plan.
   c. Administrative and personal manuals.
   d. Marketing plan.
   e. Resumes for all executive officers and department or division heads which have not been obtained in previous examinations.
   f. A list of the salary of and other compensation paid to each executive officer.
   g. A list of the salary ranges for other officers of the bank broken down by position.
   h. A description of other employee benefits.
2. Become familiar with the quality of key personnel by:
   a. Updating management briefs for all executive officers and department or division heads.
   b. Distributing the updated management briefs to appropriate examining personnel and requesting that they be returned upon completion.
3. Review administrative manuals and:
   a. Extract any policy statements contained therein.
   b. Extract any general information considered relevant in appraising management.
   c. Analyze the manual(s), in general, as useful management tools.
4. Review management plan and extract information concerning:
   a. Areas of bank where increased or decreased officer staffing is planned.
   b. Number of officers to be added or removed.
   c. Qualification requirements for planned additional officers.
5. Establish the hierarchy of the organization by determining the functional responsibility levels of various officers and whether lines of authority are drawn in accordance with the organization chart.
6. Review the bank's marketing plan for specific programs being planned and general applicability to the institution.
7. Review the bank's schedule of salaries and make comparisons with similar information from an appropriate peer group. If deemed appropriate, compare salaries paid and benefits received in the bank to those of other institutions with which it competes directly. Determine whether the bank is paying salaries or bonuses to inactive officers or directors and, if so, determine that such payments have been disclosed to shareholders.
8. Determine whether any executive incentive compensation plans (performance bonuses) have been established and, if so;
   a. Review specific provisions of the plans and determine the beneficiaries.
   b. Review controls established to prevent the beneficiary(s) of the plan from understating noncash expenses (accrual expense accounts, provision for possible loan losses, etc.) or overstating noncash income (accrual income accounts).
9. Review the bank's activities with regard to developing personnel for senior management succession. At a minimum, this review should include:
   a. An assessment of the quality of lower levels of management and the potential for advancement.
   b. An assessment of the bank's officer hiring policies to determine that it is appropriate to meet the bank's current and future needs.
10. Obtain and analyze daily or other periodic reports submitted to executive management with the view of determining the usefulness of the reports in monitoring the condition and operation of the bank.
11. As the evaluation of the various areas of examination interest are being completed, discuss with assisting personnel:
    a. Any of their observations indicative of the general morale level.
    b. The technical proficiency of officers in their area.
    c. The level of direct impact that officers have on the condition of their areas.

12. Review the section on "Analytical Review and Income and Expense" and extract any information related to financial planning that is considered relevant to evaluating management. Also consider the quality, depth and applicability of financial planning.
13. In conjunction with reviewing the work papers and comments generated during the examination:
    a. Familiarize yourself with the bank's written objectives and policies.
    b. Analyze those policies and determine any inconsistencies in management areas.
    c. Review any internal control and policy exceptions and any other criticisms made in connection with the examination of all areas of the bank.
    d. Determine the extent to which improper implementation is negating the effect of written policies and procedures.
    e. Review the appropriateness of asset distribution in view of the bank's sources of funds.
    f. Review the evaluation of the bank's capital position and expectations in view of asset quality and plans for growth and expansion.
14. In cases where previously obtained information is incomplete or where no records could be reviewed, interview appropriate management in order to judge quality and depth. The interview should be conducted in such a manner as to generate necessary information for determining:
    a. Sources of information used to keep current.
    b. Stengths and weaknesses of lower level personnel.
    c. Succession of management and replacement of key personnel.
    d. General management plan.
    e. Methods of control utilized.
    f. Workload factors and efficiency of personnel.
    g. Frequency of staff meetings and how the communications system works.
    h. Management projections for the institution over the next year.
    i. Any major new proposal being considered or changes in asset mix or services.
    j. The nature and degree of working relationship with directors.
    k. The existence of any time-consuming outside activities of executive management.
15. By reviewing the results of the preceding steps and performing any other procedures deemed appropriate, answer the following questions (normally these questions will serve as a summary of information obtained, thus compiling factual data to support your objective comments on management):
    a. Have overall management objectives been set?
    b. Does the bank forecast manpower requirements?
    c. Are qualified people advanced from within?
    d. Are supervisory personnel involved in the selection of new employees and given the right of acceptance or rejection?
    e. Is management training given to those persons likely to assume higher level positions?
    f. Are salaries competitive?
    g. Are employee benefit programs competitive?
16. Prepare comments on the quality of management supervision. The comments should, at a minimum, discuss the following:
    a. General and technical ability.
    b. Effectiveness.
    c. Experience.
    d. Any inconsistencies in written objectives, policies and procedures.
    e. Any serious or widespread lack of proper implementation of written procedures.
    f. An evaluation of the bank's salary structure.
    g. The promptness with which management addresses problems.
    h. The extent to which executive management delegates and demands accountability.
    i. Any evidence that executive management is more concerned with the operation of a functional area than with overall supervision of the bank.
    j. The potential for upward movement of existing management personnel.
    k. Management's commitment to effecting corrective action in problem areas.
    l. Unsafe or unsound management.
    m. Any situation which might require close monitoring or removal of management.

17. For banks that are subsidiaries of bank holding companies (BHCs), review the relative degree of centralized control by parent or the lead bank, and evaluate:
    a. The general level of management's dependence on central BHC staff.
    b. Independence on final credit decisions.
    c. Independence on investment decisions.
    d. Independence on operational practices or service fee arrangements.

    While examiners may expect that economies of scale or optimization of tax, investment, or credit considerations on a consolidated basis may be beneficial to the entire organization, examiners must be alert to the danger of such considerations becoming overly burdensome or unfair to the subsidiary bank being examined. (Reference Federal Reserve Policy Statement on Intercorporate Income Tax Accounting Transactions of Bank Holding Companies and State Member Banks.)

18. Update the workpapers with any information that will facilitate future examinations.

1. Does the bank have an organizational chart?
2. If not, have lines of authority and reporting responsibility been formally established?
3. Does the bank have a full-time personnel manager?
4. Does the bank utilize written personnel manuals?
5. Does the bank utilize a system of written job descriptions, including descriptions for supervisory personnel?
6. Does the bank actively recruit personnel?
7. Does the bank perform background investigations of new employees?
8. Does the bank have a formal training program?
9. Does the bank utilize other than on-the-job training?
10. Does the bank utilize a graded salary scale?
11. Does the bank consider competition in preparing a salary range? If so, in what manner?
12. Does the top management at least annually review lower management?
13. Does the bank prepare or utilize a long-range forecast of economic conditions germane to its trade area?
14. Does top management consult with directors for their opinion of future condition?
15. Does the bank either employ an economist or utilize the services of an outside economic advisor?
16. Does senior management propose to the directors areas for policy decision?
17. Does the bank have a management succession plan?
18. Does the bank employ a marketing manager and/or outside marketing consultant?
19. Does senior management receive:
    a. A brief statement of condition daily?
    b. A daily liquidity report?
    c. A listing of assets subject to quality limitations at least monthly?
    d. An earnings statement on a comparative basis at least monthly?
20. Does the bank's auditing function audit the officer's adherence to general policy?
21. Are staff meetings held on a regular basis?
22. Are minutes kept for staff meetings?
23. Does the bank use a system of progress reports on specific projects?
24. Does the bank have a tax department or a tax consultant?

Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion

Effective date October 2023

Section 4011.1

INTRODUCTION AND APPLICABILITY

This section conveys the supervisory guidance that is attached to SR-16-11, "Supervisory Guidance for Assessing Risk Management at Supervised Institutions with Total Consolidated Assets Less than $100 Billion." The guidance in SR-16-11 applies to the supervision of Federal Reserve regulated institutions with total consolidated assets less than $100 billion, which includes state member banks, bank holding companies, savings and loan holding companies (including insurance and commercial savings and loan holding companies), as well as foreign banking organizations (FBOs) with consolidated U.S. assets of less than $100 billion. This guidance is not applicable to intermediate holding companies of foreign banking organizations established pursuant to the Federal Reserve's Regulation YY with total consolidated assets of $50 billion or more.

OVERVIEW

Managing risks is fundamental to the business of banking. Accordingly, the Federal Reserve places significant supervisory emphasis on an institution's management of risk, including its system of internal controls, when evaluating the overall effectiveness of an institution's risk management. An institution's failure to establish a management structure that adequately identifies, measures, monitors, and controls the risks of its activities has long been considered unsafe and unsound conduct. Principles of sound management should apply to the entire spectrum of risks facing an institution including, but not limited to, credit, market, liquidity, operational, compliance, and legal risk:

- *Credit risk* arises from the potential that a borrower or counterparty will fail to perform on an obligation.
- *Market risk* is the risk to a financial institution's condition resulting from adverse movements in market rates or prices, including, but not limited to, interest rates, foreign exchange rates, commodity prices, or equity prices.
- *Liquidity risk* is the potential that a financial institution will be unable to meet its obligations as they come due because of an inability to liquidate assets or obtain adequate funding (referred to as "funding liquidity risk") or that it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions (referred to as "market liquidity risk").
- *Operational risk* is the risk resulting from inadequate or failed internal processes, people, and systems or from external events (this definition conforms to the Basel committee's definition of operational risk).
- *Compliance risk* is the risk of regulatory sanctions, fines, penalties or losses resulting from failure to comply with laws, rules, regulations, or other supervisory requirements applicable to a financial institution.
- *Legal risk* is the potential that actions against the institution that result in unenforceable contracts, lawsuits, legal sanctions, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a financial institution.

These risks and the activities associated with them are addressed in greater detail in the Federal Reserve's supervision manuals and other guidance documents.[1] In practice, an institution's business activities present various combinations, concentrations, and interrelationships of these risks depending on the nature and scope of the particular activity. This section provides guidelines for supervisory assessment of the overall effectiveness of an institution's risk management and its formal or informal systems for identifying, measuring, monitoring, and controlling these risks.

1. Refer to the Federal Reserve's *Commercial Bank Examination Manual*, *Bank Holding Company Supervision Manual*, *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations,* and relevant Federal Financial Institutions Examination Council Examination Manuals.

ELEMENTS OF RISK MANAGEMENT

As part of the risk management evaluation of overall management effectiveness at an institution, examiners should place primary consideration on findings relating to the following elements of a sound risk management system:

- board and senior management oversight[2]
- policies, procedures, and limits
- risk monitoring and management information systems
- internal controls

Each of these elements is described further, along with a list of considerations relevant to assessing each element. Examiners should recognize that the considerations specified in these guidelines are intended only to assist in the evaluation of risk management practices and are not a checklist of requirements for each institution.

An institution's risk management processes are expected to evolve in sophistication, commensurate with the institution's asset growth, complexity, and risk. At a larger or more complex organization, the institution should have more sophisticated risk management processes that address the full range of risks regardless of where the activity is conducted in the organization. Moreover, while a holding company should be able to assess the major risks of the consolidated organization, examiners should expect a parent company that centrally manages the operations and functions of its subsidiary banks to have more comprehensive, detailed, and developed risk management systems than a parent company that delegates the management of risks to relatively autonomous subsidiaries.[3]

For a small community banking organization (CBO) engaged solely in traditional banking activities and whose senior management is actively involved in the details of day-to-day operations, relatively basic risk management systems may be adequate. In accordance with the *Interagency Guidelines Establishing Standards for Safety and Soundness*, a CBO is expected, at a minimum, to have internal controls, information systems, and internal audit that are appropriate for the size of the institution and the nature, scope, and risk of its activities.[4]

The risk management processes of a regional banking organization (RBO) would typically contain detailed guidelines that set specific prudent limits on the principal types of risks relevant to a RBO's consolidated activities. Furthermore, because of the diversity and the geographic dispersion of their activities, these institutions will require relatively more sophisticated information systems that provide management with timely information that supports the management of risks. The information systems, in turn, should provide management with information that present a consolidated and integrated view of risks that are relevant to the duties and responsibilities of individual managers, senior management, and the board of directors.[5]

Consistent with the principle of national treatment, the Federal Reserve has the same supervisory goals and standards for the U.S. operations of FBOs as for domestic organizations of similar size, scope, and complexity.[6] Given the added element of foreign ownership, an FBO's risk management processes and control functions for the U.S. operations may be implemented domestically or outside of the United States. In cases where these functions are performed outside of the United States, the FBO's oversight function, policies and procedures, and information systems need to be sufficiently transparent to allow U.S. supervisors to assess their adequacy. Additionally, the FBO's U.S. senior management need to demonstrate and maintain a thorough understanding of all relevant risks affecting the U.S. operations and the associated

2. For the purpose of this guidance, for foreign banking organizations, "board of directors" refers to the equivalent governing body of the U.S. operations of the FBO.

3. If these subsidiaries are regulated by another federal banking agency, Federal Reserve examiners should rely on the conclusions drawn by relevant regulators regarding risk management to the fullest extent possible. See also, SR-16-4, "Relying on the Work of the Regulators of the Subsidiary Insured Depository Institution(s) of Bank Holding Companies and Savings and Loan Holding Companies with Total Consolidated Assets of Less than $100 Billion."

4. Refer to 12 CFR 208, Appendix D-1, the Interagency Guidelines Establishing Standards for Safety and Soundness.

5. Subpart C of the Federal Reserve's Regulation YY includes risk committee requirements for bank holding companies with total consolidated assets of $50 billion or more and less than $100 billion.

6. National treatment requires nondiscrimination between domestic and foreign firms, or treatment of foreign entities that is no less favorable than that accorded to domestic enterprises in like circumstances. The International Banking Act of 1978 generally gives foreign banks operating in the United States the same powers as domestic banking organizations and subjects them to the same restrictions and obligations.

management information systems, used to manage and monitor these risks within the U.S. operations.

The information systems at a larger institution will naturally require frequent monitoring and testing by independent control areas, and by both internal and external auditors, to ensure the integrity of the information used by the board of directors and senior management in overseeing compliance with policies and limits. Therefore, an institution's risk oversight function needs to be sufficiently independent of the business lines to achieve an adequate separation of duties and the avoidance of conflicts of interest.

Board and Senior Management Oversight

The board of directors has the responsibility for establishing the level of risk that the institution should take. Accordingly, the board of directors should approve the institution's overall business strategies and significant policies, including those related to managing risks. Further, the board of directors should also ensure that senior management is fully capable of implementing the institution's business strategies and risk limits. In evaluating senior management, the board of directors should consider whether management is taking the steps necessary to identify, measure, monitor, and control these risks.

The board of directors should collectively have a balance of skills, knowledge, and experience to clearly understand the activities and risks to which the institution is exposed. The board of directors should take steps to develop an appropriate understanding of the risks the institution faces, through briefings from experts internal to their organization and potentially from external experts. The institution's management information systems should provide the board of directors with sufficient information to identify the size and significance of the risks. Using this knowledge and information, the board of directors should provide clear guidance regarding the level of exposures acceptable to the institution and oversee senior management's implementation of the procedures and controls necessary to comply with approved policies.

Senior management is responsible for implementing strategies set by the board of directors in a manner that controls risks and that complies with laws, rules, regulations, or other supervisory requirements on both a long-term and day-to-day basis. Accordingly, senior management should be fully involved in and possess sufficient knowledge of all activities to ensure that appropriate policies, controls, and risk monitoring systems are in place and that accountability and lines of authority are clearly delineated. Senior management is also responsible for establishing and communicating a strong awareness of the need for effective risk management, internal controls, and high ethical business practices. To fulfill these responsibilities, senior management needs to have a thorough understanding of banking and financial market activities and detailed knowledge of the institution's activities, including the internal controls that are necessary to limit the related risks.

In assessing the quality of the oversight provided by the board of directors and senior management, examiners should consider the following:

- The board of directors has approved significant policies to establish risk tolerances for the institution's activities and periodically reviews risk exposure limits to align with changes in the institution's strategies, address new activities and products, and react to changes in the industry and market conditions.
- Senior management has identified and has a clear understanding and working knowledge of the risks inherent in the institution's activities. Senior management also remains informed about these risks as the institution's business activities evolve or expand and as changes and innovations occur in financial markets and risk management practices.
- Senior management has identified and reviewed risks associated with engaging in new activities or introducing new products to ensure that the necessary infrastructure and internal controls are in place to manage the related risks.
- Senior management has ensured that the institution's activities are managed and staffed by personnel with the knowledge, experience, and expertise consistent with the nature and scope of the institution's activities and risks.
- All levels of senior management provide appropriate management of the day-to-day activities of officers and employees, including oversight of senior officers or heads of business lines.
- Senior management has established and maintains effective information systems to identify, measure, monitor, and control the sources of risks to the institution.

Policies, Procedures, and Limits

Although an institution's board of directors approves an institution's overall business strategy and policy framework, senior management develops and implements the institution's risk management policies and procedures that address the types of risks arising from its activities. Once the risks are properly identified, the institution's policies and procedures should provide guidance for the day-to-day implementation of business strategies, including limits designed to prevent excessive and imprudent risks. An institution should have policies and procedures that address its significant activities and risks with the appropriate level of detail to address the type and complexity of the institution's operations. A smaller, less complex institution that has effective senior management directly involved in day-to-day operations would generally not be expected to have policies as sophisticated as larger institutions. In a larger institution, where senior managers rely on widely dispersed staffs to implement strategies for more varied and complex businesses, far more detailed policies and procedures would generally be expected. In either case, senior management is expected to ensure that policies and procedures address the institution's material areas of risk and that policies and procedures are modified when necessary to respond to significant changes in the institution's activities or business conditions.

The following guidelines should assist examiners in evaluating an institution's policies, procedures, and limits:

- The institution's policies, procedures, and limits provide for adequate identification, measurement, monitoring, and control of the risks posed by its significant risk-taking activities.
- The policies, procedures, and limits are consistent with the institution's stated strategy and risk profile.
- The policies and procedures establish accountability and lines of authority across the institution's activities.
- The policies and procedures provide for the review and approval of new business lines, products, and activities, as well as material modifications to existing activities, services, and products, to ensure that the institution has the infrastructure necessary to identify, measure, monitor, and control associated risks before engaging in a new or modified business line, product, or activity.

Risk Monitoring and Management Information Systems

Institutions of all sizes are expected to have risk monitoring and management information systems in place that provide the board of directors and senior management with timely information and a clear understanding of the institution's business activities and risk exposures. The sophistication of risk monitoring and management information systems should be commensurate with the complexity and diversity of the institution's operations. Accordingly, a smaller and less complex institution may require less frequent management and board reports to support risk monitoring activities. For example, these reports may include, daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report on past due loans, an interest rate risk report, and similar items. In contrast, a larger, more complex institution would be expected to have much more comprehensive reporting and monitoring systems, which includes more frequent reporting to board and senior management, tighter monitoring of high-risk activities, and the ability to aggregate risks on a fully consolidated basis across all business lines, legal entities, and activities.

In assessing an institution's measurement and monitoring of risk and its management reports and information systems, examiners should consider whether these conditions exist:

- The institution's risk monitoring practices and reports address all of its material risks.
- Key assumptions, data sources, models, and procedures used in measuring and monitoring risks are appropriate and adequately documented and tested for reliability on an on-going basis.[7]
- Reports and other forms of communication address the complexity and range of an institution's activities, monitor key exposures and compliance with established limits and strategy, and as appropriate, compare actual versus expected performance.
- Reports to the board of directors and senior management are accurate, and provide timely and sufficient information to identify any adverse trends and to evaluate the level of risks faced by the institution.

7. See this manual's section "Model Risk Management," and SR-11-7, "Guidance on Model Risk Management."

Internal Controls

An effective internal control structure is critical to the safe and sound operation of an institution. Effective internal controls promote reliable financial and regulatory reporting, safeguard assets, and help to ensure compliance with relevant laws, rules, regulations, supervisory requirements, and institutional policies. Therefore, an institution's senior management is responsible for establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate segregation of duties.

Adequate segregation of duties is a fundamental and essential element of a sound risk management and internal control system. Failure to implement and maintain an adequate segregation of duties can constitute an unsafe and unsound practice and possibly lead to serious losses or otherwise compromise the integrity of the institution's internal controls. Serious lapses or deficiencies in internal controls, including inadequate segregation of duties, may warrant supervisory action, including formal enforcement action.

Internal controls should be tested by an independent party who reports either directly to the institution's board of directors or its designated committee, which is typically the audit committee.[8] However, small CBOs whose size and complexity do not warrant a full scale internal audit function may rely on regular reviews of essential internal controls conducted by other institution personnel. Given the importance of appropriate internal controls to institutions of all sizes and risk profiles, the results of audits or reviews, whether conducted by an internal auditor or by other personnel, should be adequately documented, as should management's responses to the findings. In addition, communication channels should allow for adverse or sensitive findings to be reported directly to the board of directors or to the relevant board committee.

In evaluating internal controls, examiners should consider whether these conditions are met:

- The system of internal controls is appropriate to the type and level of risks posed by the nature and scope of the institution's activities.
- The institution's organizational structure establishes clear lines of authority and responsibility for risk management and for monitoring adherence to policies, procedures, and limits.
- Internal audit or other control functions, such as loan review and compliance, provide for independence and objectivity.
- The official organizational structures reflect actual operating practices and management responsibilities and authority over a particular business line or activity.
- Financial, operational, risk management, and regulatory reports are reliable, accurate, and timely; and wherever applicable, material exceptions are noted and promptly investigated or remediated.
- Policies and procedures for control functions support compliance with applicable laws, rules, regulations, or other supervisory requirements.
- Internal controls and information systems are adequately tested and reviewed; the coverage, procedures, findings, and responses to audits, regulatory examinations, and other review tests are adequately documented; identified material weaknesses are given appropriate and timely, high-level attention; and management's actions to address material weaknesses are objectively verified and reviewed.
- The institution's board of directors, or audit committee, and senior management are responsible for developing and implementing an effective system of internal controls and that the internal controls are operating effectively.

Conclusions

Examiners are expected to assess risk management for an institution and assign formal ratings of "risk management" as described in this manual for state member banks, the *Bank Holding Company Manual* for holding companies, and the *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations*.[9] In

8. Given the importance of the internal audit function, several additional policy statements have been issued. For comprehensive guidance on internal audit, see SR-03-5, "Amended Interagency Guidance on the Internal Audit Function and its Outsourcing" and for institutions with more than $10 billion in assets, see SR-13-1/ CA-13-1, "Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing."

9. Refer to the section entitled, "Overall Conclusions Regarding Condition of the Bank: Uniform Financial Institutions Rating System and the Federal Reserve's Risk Management Rating," of this manual; the RFI Ratings section of the *Bank Holding Company Supervision Manual*; and the "Rating System for U.S. Branches and Agencies of Foreign Banking

reports of examination or inspection, and in transmittal letters to the boards of directors of state member banks, holding companies, and to the FBO officer of the U.S. operations, examination staff should specifically reference the types and nature of corrective actions that need to be taken by an institution to address noted risk management and internal control deficiencies. Where appropriate, the Federal Reserve will advise an institution that supervisory action will be initiated, if the institution fails to timely remediate risk management weaknesses when such failures create the potential for serious losses or if material deficiencies or situations threaten its safety and soundness. Such supervisory actions may include formal enforcement actions against the institution, or its responsible officers and directors, or both, and would require the immediate implementation of all necessary corrective measures.

If bank or holding company subsidiaries are regulated by another federal banking agency, Federal Reserve examiners should rely to the fullest extent possible on the conclusions drawn by relevant regulators regarding risk management. See also, SR-16-4, "Relying on the Work of the Regulators of the Subsidiary Insured Depository Institution(s) of Bank Holding Companies and Savings and Loan Holding Companies with Total Consolidated Assets of Less than $100 Billion."

Organizations" section of the *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations*. For relevant savings and loan holding companies, see the RFI Ratings section of the *Bank Holding Company Supervision Manual* and SR-14-9, "Incorporation of Federal Reserve Policies into the Savings and Loan Holding Company Supervision Program."

Risk-Management Processes and Internal Controls of Firms Having $100 Billion or More in Total Assets

Effective date October 2023

Section 4012.1

APPLICABILITY

The guidance in this section largely is based on SR-95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies." This risk management guidance applies to the supervision of state member banks and bank holding companies with greater than $100 billion in total consolidated assets.

SR-95-51 instituted an explicit risk-management rating requirement to be assigned for examinations commencing on or after January 2, 1996. The risk-management rating applies to all state member banks, regardless of their size. For more information on this risk-management rating, see this manual's section entitled, "Uniform Financial Institutions Rating System and the Federal Reserve's Risk Management Rating."

INTRODUCTION

The Federal Reserve places significant supervisory emphasis on the adequacy of an institution's management of risk, including its system of internal controls, when assessing the condition of an organization. An institution's failure to establish a management structure that adequately identifies, measures, monitors, and controls the risks involved in its various products and lines of business has long been considered unsafe-and-unsound conduct. Principles of sound management should apply to the entire spectrum of risks facing a banking institution, including, but not limited to, credit, market, liquidity, operational, and legal risk.

- *Credit risk* arises from the potential that a borrower or counterparty will fail to perform on an obligation.
- *Market risk* is the risk to a financial institution's condition resulting from adverse movements in market rates or prices, such as interest rates, foreign exchange rates, or equity prices.
- *Liquidity risk* is the potential that an institution will be unable to meet its obligations as they come due because of an inability to liquidate assets or obtain adequate funding (referred to as "funding liquidity risk"), or that it cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions (referred to as "market liquidity risk").
- *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.
- *Legal risk* arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of an institution.

ELEMENTS OF RISK MANAGEMENT

When evaluating the quality of risk management as part of the evaluation of the overall quality of management, examiners should place primary consideration on findings relating to the following elements of a sound risk-management system:

- active board and senior management oversight
- adequate policies, procedures, and limits
- adequate risk measurement, risk monitoring, and management information systems
- comprehensive internal controls

Examiners should recognize that the considerations specified in these guidelines are intended only to assist in the evaluation of risk-management practices, and not as a checklist of requirements for each institution. Moreover, while all bank holding companies should be able to assess the major risks of the consolidated organization, examiners should expect parent companies that centrally manage the operations and functions of their subsidiary banks to have more comprehensive, detailed, and developed risk-management systems than companies that delegate the management of risks to relatively autonomous banking subsidiaries.

Adequate risk-management programs can vary considerably in sophistication, depending on the size and complexity of the institution and the level of risk that it accepts. For smaller institu-

tions engaged solely in traditional banking activities and whose senior managers and directors are actively involved in the details of day-to-day operations, relatively basic risk-management systems may be adequate. In such institutions, these systems may consist only of written policies addressing material areas of operations, such as lending or investing, basic internal control systems, and a limited set of management and board reports. However, large, multinational organizations will require far more elaborate and formal risk-management systems to address their broader and typically more-complex range of financial activities, and to provide senior managers and directors with the information they need to monitor and direct day-to-day activities. In addition to the banking organization's market and credit risks, risk-management systems should encompass the organization's trust and fiduciary activities, including investment advisory services, mutual funds, and securities lending.

The risk-management processes of large banking organizations would typically contain detailed guidelines that set specific prudential limits on the principal types of risks relevant to their activities worldwide. Furthermore, because of the diversity of their activities and the geographic dispersion of their operations, these institutions will require timely and relatively more sophisticated reporting systems in order to manage their risks properly. These reporting systems, in turn, should comprise an adequate array of reports that provide the levels of detail about risk exposures that are relevant to the duties and responsibilities of individual managers and directors.

Such extensive systems of large institutions will naturally require frequent monitoring and testing by independent control areas and internal, as well as external, auditors to ensure the integrity of the information used by senior officials in overseeing compliance with policies and limits. The risk-management systems or units of such institutions must also be sufficiently independent of the business lines in order to ensure an adequate separation of duties and the avoidance of conflicts of interest.

Board Oversight and the Role of Senior Management

Boards of directors have ultimate responsibility for the level of risk taken by their institutions. Accordingly, they should approve the overall business strategies and significant policies of their organizations, including those related to managing and taking risks, and should also ensure that senior management is fully capable of managing the activities that their institutions conduct. While all boards of directors are responsible for understanding the nature of the risks significant to their organizations and overseeing and holding senior management accountable for maintaining an effective risk-management framework, the level of technical knowledge required of directors may vary depending on the particular circumstances at the institution.

Directors of large banking organizations that conduct a broad range of technically complex activities, for example, cannot be expected to understand the full details of their institutions' activities or the precise ways risks are measured and controlled. They should, however, have a clear understanding of the types of risks to which their institutions are exposed and senior management should provide reports to the board of directors that identify and summarize the size, complexity, and significance of the risks in terms that are meaningful to them. In fulfilling this responsibility, directors should take steps to develop an appropriate understanding of the risks their institutions face, possibly through briefings from auditors and experts external to the organization. Using this knowledge and information, directors should provide clear guidance regarding the level of exposures acceptable to their institutions and have the responsibility to ensure that senior management implements the procedures and controls necessary to comply with adopted policies.

Directors of institutions that conduct more traditional and less complicated business activities may require significantly less knowledge of complex financial transactions or capital markets.

Senior management is responsible for implementing strategies in a manner that manages, monitors, and mitigates risks associated with each strategy and that ensures compliance with laws and regulations on both a long-term and day-to-day basis. Accordingly, senior management should be fully involved in the activities of

their institutions and possess sufficient knowledge of all major business lines to ensure that appropriate policies, controls, and risk monitoring systems are in place and that accountability and lines of authority are clearly delineated. Senior management is also responsible for establishing and communicating a strong awareness of and need for effective internal controls and high ethical standards. Meeting these responsibilities requires senior managers of a bank or bank holding company to have a thorough understanding of banking and financial market activities and detailed knowledge of the activities their institution conducts, including the nature of internal controls necessary to limit the related risks.

When assessing the quality of the oversight by boards of directors and the managing, monitoring, and mitigating of risk by senior management, examiners should consider whether the institution follows policies and practices such as those described below:

- The board makes appropriate efforts to remain informed about risks inherent to the institution's activities and holds senior management accountable as financial markets, risk-management practices, and the bank holding company's activities evolve.
- The board reviews and approves significant policies to limit risks inherent in the institution's lending, investing, trading, trust, fiduciary, and other significant activities or products.
- The board reviews and approves significant risk-exposure limits to conform to any changes in the institution's strategies, reviews new products, and reacts to changes in market conditions.

- Senior management have identified and have a clear understanding and working knowledge of the types of risks inherent in the institution's activities, and they make appropriate efforts to remain informed about these risks as financial markets, risk-management practices, and the institution's activities evolve.
- Senior management is sufficiently familiar with and is using adequate recordkeeping and reporting systems to measure and monitor the major sources of risk to the organization.
- Senior management ensures that its lines of business are managed and staffed by personnel whose knowledge, experience, and expertise is consistent with the nature and scope of the banking organization's activities.
- Senior management ensures that the depth of staff resources is sufficient to operate and soundly manage the institution's activities, and ensures that employees have the integrity, ethical values, and competence that are consistent with a prudent management philosophy and operating style.
- Senior management at all levels provides adequate supervision of the day-to-day activities of officers and employees, including management supervision of senior officers or heads of business lines.
- Senior management is able to respond to risks that may arise from changes in the competitive environment or from innovations in markets in which the organization is active.
- Before embarking on new activities or introducing new products, senior management identifies and reviews all risks associated with the activities or products and ensures that the infrastructure and internal controls necessary to manage the related risks are in place.

Adequate Policies, Procedures, and Limits

An institution's directors should set clear, aligned, and consistent direction regarding the firm's strategy and risk appetite. Once risks are properly identified, the institution's policies and its fully articulated procedures provide detailed guidance for the day-to-day implementation of broad business strategies, and generally include limits designed to shield the organization from excessive and imprudent risks. While all banking organizations should have policies and procedures that address their significant activities and risks, the coverage and level of detail embodied in these statements will vary among institutions. A smaller, less complex institution that has effective management that is heavily involved in day-to-day operations generally would be expected to have only basic policies addressing the significant areas of operations and setting forth a limited set of requirements and procedures. In a larger institution, where senior managers must rely on widely dispersed staffs to implement strategies in an extended range of potentially complex businesses, more detailed policies and related procedures would generally be expected. In either case, however, senior management is expected to ensure that policies and procedures address the material areas of risk

to an institution and that they are modified when necessary to respond to significant changes in the banking organization's activities or business conditions.

Examiners should consider the following when evaluating the adequacy of a banking organization's policies, procedures, and limits:

- The institution's policies, procedures, and limits provide for adequate identification, measurement, monitoring, and control of the risks posed by its lending, investing, trading, trust, fiduciary, and other significant activities.
- The policies, procedures, and limits are consistent with senior management's experience level, the institution's stated goals and objectives, and the overall financial strength of the organization.
- Policies clearly delineate accountability and lines of authority across the institution's activities.
- Policies provide for the review of new activities to ensure that the financial institution has the necessary infrastructures to identify, monitor, and control risks associated with an activity before it is initiated.

Adequate Risk Monitoring and Management Information Systems

Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk monitoring activities must be supported by information systems that provide senior managers and directors with timely reports on the financial condition, operating performance, and risk exposure of the consolidated organization as well as with regular and sufficiently detailed reports for line managers engaged in the day-to-day management of the organization's activities.

The sophistication of risk monitoring and management information systems should be consistent with the complexity and diversity of the institution's operations. Accordingly, smaller and less complicated banking organizations may require only a limited set of management and board reports to support risk monitoring activities. These reports include, for example, daily or weekly balance sheets and income statements, a watch list for potentially troubled loans, a report for past due loans, a simple interest rate risk report, and similar items. Larger, more complicated institutions, however, would be expected to have much more comprehensive reporting and monitoring systems that allow, for example, for more frequent reporting, tighter monitoring of complex trading activities, and the aggregation of risks on a fully consolidated basis across all business lines and activities. Financial institutions of all sizes are expected to have risk monitoring and management information systems in place that provide directors and senior management with a clear understanding of the banking organization's positions and risk exposures.

When assessing the adequacy of an institution's risk measurement and monitoring, as well as its management reports and information systems, examiners should consider whether these conditions exist:

- The institution's risk monitoring practices and reports address all of its material risks.
- Key assumptions, data sources, and procedures used in measuring and monitoring risk are appropriate and adequately documented, and are tested for reliability on an ongoing basis.
- Reports and other forms of communication are consistent with the banking organization's activities; are structured to monitor exposures and compliance with established limits, goals, or objectives; and, as appropriate, compare actual versus expected performance.
- Reports to senior management or to the institution's directors are accurate and timely, and contain sufficient information for decision makers to identify any adverse trends and to evaluate adequately the level of risk faced by the institution.

Adequate Internal Controls

An institution's internal control structure is critical to the safe-and-sound functioning of the organization generally and to its risk-management system, in particular. Establishing and maintaining an effective system of controls, including the enforcement of official lines of authority and the appropriate separation of duties—such as trading, custodial, and back-office—is one of management's more important responsibilities.

Appropriately segregating duties is a fundamental and essential element of a sound risk management and internal control system. Failure to implement and maintain an adequate separation of duties can constitute an unsafe-

and-unsound practice and possibly lead to serious losses or otherwise compromise the financial integrity of the institution. Serious lapses or deficiencies in internal controls, including inadequate segregation of duties, may warrant supervisory action, including formal enforcement action.

When properly structured, a system of internal controls promotes effective operations and reliable financial and regulatory reporting, safeguards assets, and helps to ensure compliance with relevant laws, regulations, and institutional policies. Ideally, internal controls are tested by an independent internal auditor who reports directly either to the institution's board of directors or its designated committee, which is typically the audit committee. However, smaller institutions whose size and complexity do not warrant a full-scale internal audit function may rely on regular reviews of essential internal controls conducted by other institution personnel. Personnel performing these reviews generally should be independent of the function they are assigned to review. Given the importance of appropriate internal controls to banking organizations of all sizes and risk profiles, the results of audits or reviews, whether conducted by an internal auditor or by other personnel, should be adequately documented, as should senior management's responses to them. In addition, communication channels should exist that allow negative or sensitive findings to be reported directly to the board of directors or to the relevant board committee.

When evaluating the adequacy of a financial institution's internal controls and audit procedures, examiners should consider whether these conditions are met:

- The system of internal controls is appropriate to the type and level of risks posed by the nature and scope of the organization's activities.
- The institution's organizational structure establishes clear lines of authority and responsibility for monitoring adherence to policies, procedures, and limits.
- Reporting lines for the control areas are independent from the business lines, and there is adequate separation of duties throughout the organization—such as duties relating to trading, custodial, and back-office activities.
- Official organizational structures reflect actual operating practices.
- Financial, operational, and regulatory reports are reliable, accurate, and timely, and, when applicable, exceptions are noted and promptly investigated.
- Adequate procedures exist for ensuring compliance with applicable 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. The coverage of, procedures for, and findings and responses to audits and review tests are adequately documented. Identified material weaknesses are given appropriate and timely high-level attention, and management's actions to address material weaknesses are objectively verified and reviewed.
- The institution's audit committee or board of directors engages in robust inquiry into the effectiveness of internal audits and other control-review activities regularly.

The risk-management rating is to be reflected in the institution's overall "Management" rating. The risk-management rating should be consistent with the stated rating criteria of "1" through "5." For more information see the section entitled, "Uniform Financial Institutions Rating System and the Federal Reserve's Risk Management Rating."

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

INTRODUCTION—PART I

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

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

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

PURPOSE AND SCOPE—PART II

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

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

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

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

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

OVERVIEW OF MODEL RISK MANAGEMENT—PART III

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

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

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

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

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

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

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

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

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

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

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

MODEL DEVELOPMENT, IMPLEMENTATION, AND USE—PART IV

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

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

Model Development and Implementation

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

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

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

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

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

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

appropriate and systematic manner and are well documented.

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

Model Use

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

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

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

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

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

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

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

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

MODEL VALIDATION—PART V

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

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

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

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

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

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

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

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

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

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

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

Key Elements of Comprehensive Validation

An effective validation framework should include three core elements:

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

Evaluation of Conceptual Soundness

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

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

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

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

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

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

Ongoing Monitoring

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

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

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

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

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

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

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

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

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

Outcomes Analysis

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

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

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

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

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

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

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

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

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

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

Validation of Vendor and Other Third-Party Products

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

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

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

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

GOVERNANCE, POLICIES, AND CONTROLS—PART VI

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

Board of Directors and Senior Management

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

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

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

Policies and Procedures

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

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

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

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

Roles and Responsibilities

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

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

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

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

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

Internal Audit

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

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

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

External Resources

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

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

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

Model Inventory

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

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

Documentation

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

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

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

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

CONCLUSION—PART VII

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

INTRODUCTION

Asset securitization typically involves the transfer of potentially illiquid on-balance-sheet assets (for example, mortgages, loans, leases) to a third party or trust. In turn, the third party or trust issues certificates or notes to investors. The cash flow from the transferred assets supports repayment of the certificates or notes. Firms use asset securitization to access alternative funding sources, manage loan concentrations, improve financial-performance ratios, and more efficiently meet customers' financing needs. Assets that are typically securitized include credit card receivables, automobile receivable paper, commercial or residential first-priority mortgages, commercial loans, home-equity loans, and student loans.

WHY FIRMS ENGAGE IN SECURITIZATION ACTIVITIES

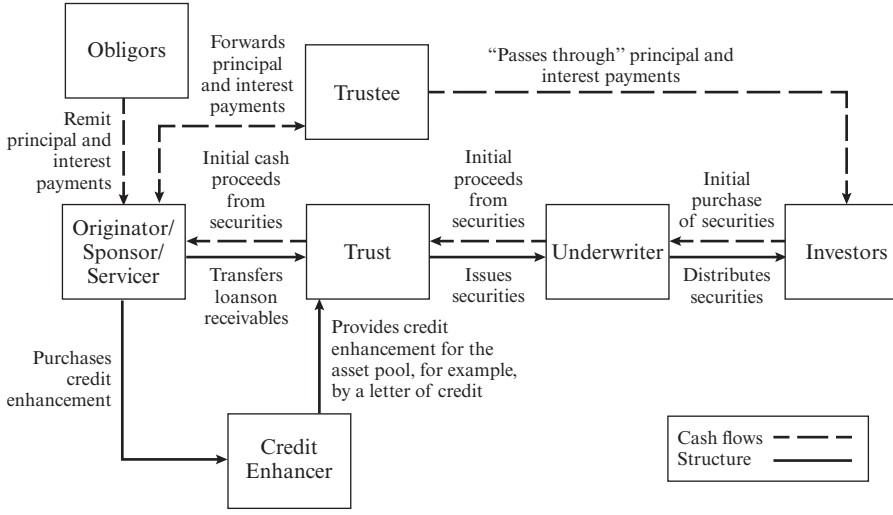
While the objectives of securitization may vary, securitized transactions may provide several benefits, such as

- transferring some of a firm's risks of ownership to parties willing and able to manage the risk;
- improving a firm's ability to manage potential asset-liability mismatches and credit concentrations;
- reducing a firm's interest-rate risk by improving the firm's asset-liability mix, especially if the firm has a large investment in fixed-rate, low-yield assets;
- transferring some on-balance-sheet assets to off-balance-sheet assets to provide some cost savings of on-balance sheet financing and enhances the firm's returns on equity and assets; or
- allowing a firm to convert its illiquid assets into a security with greater marketability that can be sold and used to diversify a firm's funding base at a potentially more favorable rate of return.

THE SECURITIZATION PROCESS

As depicted in figure 1, the asset-securitization process begins with the segregation of assets into pools that are relatively homogeneous with

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



respect to credit, maturity, and interest-rate risks. These pools of assets are then transferred to a trust or other entity known as "an issuer" because the entity issues the securities or ownership interests that will be acquired by investors. These asset-backed securities (ABS) may take the form of debt, certificates of beneficial ownership, or other financial instruments. The issuer is typically protected from bankruptcy through various structural and legal arrangements. A sponsor of the securitization provides the assets to be securitized (which may or may not have been originated by the sponsor) and owns or otherwise establishes the issuer.

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

The structure of the ABS also may include a guarantor that ensures that investors receive principal and interest payments on the securities on a timely basis. The guarantor agrees to make these payments to investors even if the servicer cannot collect these payments from the obligors of the underlying assets. Many issuances of mortgage-backed securities are guaranteed directly by the Government National Mortgage Association (GNMA or Ginnie Mae), which is backed by the full faith and credit of the U.S. government. Privately issued mortgage-backed securities and other types of ABS may depend on some form of credit enhancement provided by the originator of the assets or a third party to insulate the investor from some portion of, or all, credit losses. The amount of the credit enhancement may be based on several multiples of the historical losses experienced on the particular assets backing the security.

The structure of an ABS and the terms of the investors' interest(s) in the underlying assets backing the security can vary widely depending on the type of assets, the risk tolerance(s) and investment objective(s) of the investors, and the use of credit enhancements. Securitizations typically divide the credit risk of the underlying assets into different levels (sometimes called "tranches") of risk–return properties and distribute it based on the risk tolerance(s) of investors. The *first-dollar* loss, or most subordinate, position is the first to absorb credit losses, and the most senior investor position is the last to absorb losses. There also may be one or more loss positions between those tranches. Each loss position functions as a credit enhancement for the more senior positions in the structure. In other words, when ABS reallocate the risks in the underlying assets (particularly credit risk), the risks are moved into security tranches that match the desires of investors. For example, senior-subordinated security structures give holders of senior tranches greater credit-risk protection—albeit at lower yields—than holders of subordinated tranches. Under this structure, at least two classes of asset-backed securities—a senior and a junior (or subordinated) class—are issued in connection with the same pool of assets. The senior class is structured so that it has a priority claim on the cash flows from the underlying pool of assets. The subordinated class must absorb credit losses on the collateral before the senior portion experiences any losses.

TYPES OF ASSET-BACKED SECURITIES

Asset securitization involves different types of capital-market instruments. These instruments may be structured as "pass-throughs" or "pay-throughs."

Under a pass-through structure, the cash flows from the underlying pool of assets are passed through to investors on a pro rata or proportional basis. This type of security may be a single-class instrument, such as a GNMA pass-through, or a multiclass instrument, such as a real estate mortgage investment conduit.

The pay-through structure, which contains multiple classes, aggregates the cash flows from the underlying pool of assets and reallocates them to two or more issues of securities that have different cash-flow characteristics and maturities. While not particularly common, one example of a pay-through structure is the collateralized mortgage obligation (CMO), which has a series of bond classes, each with its own specified coupon and stated maturity. In most cases, the assets that make up the CMO collateral pools are pass-through securities. Scheduled principal payments and any prepayments from the underlying assets go first to the earliest maturing class of bonds. This first class of bonds must be retired before the principal cash flows from the assets would be used to retire the later

bond classes. The development of the pay-through structure resulted from the desire to broaden the marketability of these securities to investors who were interested in maturities other than those generally associated with pass-through securities.

ABS backed by multiple classes of securities also may be issued as derivative instruments, such as "stripped" securities. Investors in each class of a stripped security would receive a different portion of the principal and interest cash flows from the underlying pool of assets. In their purest form, stripped securities may be issued as interest-only strips, for which the investor receives 100 percent of the interest paid on the underlying pool of assets, and as principal-only strips, for which the investor receives all of the principal paid on the underlying pool of assets. Other types of financial instruments may arise as a result of asset securitization, such as

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

Asset-Backed Commercial Paper Programs

An asset-backed commercial paper (ABCP) program typically is a program through which a firm provides funding to its corporate customers by sponsoring and administering a bankruptcy-remote, special-purpose entity that purchases asset pools from, or extends loans to, those customers.[1] The underlying asset pools for an ABCP program might include, for example, trade receivables, consumer loans, or ABS. The ABCP program raises cash to provide funding to the firm's customers through the issuance of externally rated commercial paper into the market. The sponsoring firm often provides liquidity and credit enhancements to the ABCP program.

ABCP programs differ from some other methods of securitization in that ABCP programs typically include more than one type of asset in the underlying asset pool. Moreover, in certain cases, the cash flow from the asset pool may not necessarily match the payments to investors—the maturity of the underlying assets need not always parallel the maturity of the commercial paper liabilities of the ABCP program—since the ABCP program can engage in maturity transformation. In those instances, when the commercial paper issued by the ABCP program matures, that commercial paper usually is rolled over into, or otherwise funded by, another commercial paper issuance by the ABCP program.

For more information, see this manual's section entitled, "Overview of Asset-Backed Commercial Paper Programs."

RISKS ASSOCIATED WITH SECURITIZATION ACTIVITIES

The types of risks that firms encounter when engaging in securitization activities include credit risk, concentration risk, interest-rate risk (including prepayment risk), operational risk, and liquidity risk. Securitization activities have the potential to increase the overall risk profile of the firm if they are not carried out prudently. A firm's risk exposure will depend on the firm's role in the ABS, such as originator, servicer, credit

1. ABCP programs can include structured investment vehicles (entities that earn a spread by issuing commercial paper and medium-term notes and using the proceeds to purchase highly rated debt securities) and securities arbitrage programs.

enhancer, trustee, or investor. Potential risks can include the following:

- *Credit risk.* Firms should be aware that the credit risk involved in many securitization activities may not always be obvious. For certain types of loan securitizations, a firm may be exposed to essentially the same credit risk as in traditional lending activities, even though a particular transaction may appear to separate the firm from any risk exposure. In such cases, the firm's transfer of an asset from its balance sheet may not result in a commensurate reduction in its credit risk. Transactions that can give rise to such instances include loan sales with recourse; providing protection through credit derivatives; direct-credit substitutes, such as letters of credit; and liquidity facilities extended to securitization programs (for example, asset-securitization structures used to securitize credit card receivables). Deterioration of assets in a pool underlying a prior securitization may result in negative investor sentiment that could result in increased spreads for subsequent ABS issuances. To avoid potential increases in their funding costs, firms sometimes support their securitization transactions by improving the performance of the underlying asset pool (for example, by selling discounted receivables or adding higher-quality assets to the pool).
- *Concentration risk.* A firm involved in originating, packaging, servicing, underwriting, or enhancing the creditworthiness of ABS should follow its internal diversification requirements for aggregate outstanding credits to any particular institution, industry, or geographic area.
- *Liquidity and market risk.* The existence of recourse provisions in asset sales, the extension of liquidity facilities to securitization programs, and early-amortization triggers of certain ABS transactions can result in significant liquidity risk to a firm serving as sponsor or issuer for the securitization. Firms engaging in these activities should ensure that their liquidity contingency plans fully incorporate the potential risk posed by their securitization activities. Upon new issuance of ABS, a firm acting as issuer should determine the potential effect on the firm's liquidity at the inception of each transaction and throughout the life of the ABS to evaluate the firm's future funding needs.
- *Transfer risk.* Transfer risk is analogous to liquidity risk. It is the risk that a firm with obligations under securitization arrangements (for example, as liquidity provider or servicer) may wish to relinquish those obligations to another party but may not be able to do so.
- *Operational risk.* This risk arises from uncertainty about a firm's ability to meet its obligations under securitization arrangements. For instance, operational risk arises when a firm has insufficient resources to meet its contractual obligations or when its fee income is insufficient to cover the costs associated with its obligations. A firm filling a role that potentially requires long-term resource commitments, such as servicer or credit enhancer, is susceptible to an operational risk.
- *Legal risk.* When a firm plays multiple roles in securitization, conflicts of interest may arise. Policies and procedures should address any potential conflict, especially any legal risk or negative market risk that may result if the firm appears to compromise any fiduciary and contractual responsibilities to obligors or investors.

ADDITIONAL RISKS ASSOCIATED WITH SECURITIZATION ACTIVITIES

Investor-Specific Risks

Investors in ABS may be exposed to varying degrees of credit risk based on the potential for obligors of the underlying assets to default on principal and interest payments. As with direct investment in the underlying assets, an investment in ABS is subject to the risk that the various parties in the securitization structure, for example, the servicer or trustee, may not be able to fulfill their contractual obligations. Moreover, ABS investors may be susceptible to concentrations of risks across various ABS investments, such as (1) overexposure to a particular firm that performs various roles in ABS securitizations, or (2) concentrations to particular geographic exposures of the underlying asset pool(s). Also, ABS investors may face heightened liquidity risk when seeking to sell ABS compared to direct holders of the underlying assets, since the secondary markets for certain ABS may be more limited than those of the underlying asset. Furthermore, certain derivative instruments, such as stripped asset-backed securities and residuals,

may be extremely sensitive to interest rates and exhibit a relatively high degree of price volatility. Therefore, a firm investing in these instruments may face considerable volatility in its risk exposure unless it uses a properly structured hedging strategy.

Issuer-Specific Risks

Firms that issue ABS may feel conflicting pressures related to the assets to be transferred into pools for securitization: some may feel pressure to sell only their best assets into securitization pools, thus reducing the asset quality of their own loan portfolios, while others may feel they can relax their credit standards based on the belief that any higher-risk assets can be sold for securitization quickly, without risk to the firm's own portfolio. In addition, some issuers may face pressures to repurchase from a securitization any securities backed by loans or leases they previously originated that have deteriorated and become nonperforming, even if under no legal obligation to repurchase those assets (sometimes termed "moral recourse"). Issuers also may face funding risk if market conditions are not conducive to the issuance of ABS in the securitization pipeline and the firm therefore must hold the underlying assets.

Servicer-Specific Risks

Firms that service securitizations need to have policies, operations, and systems that would allow them to continue to serve as servicer without interruption and to avoid defaults. A firm can realize substantial fee income by acting as a servicer, particularly if it can leverage its fixed investment in servicing systems to achieve economies of scale. However, in seeking such scale, a firm can risk overloading its system's capacity, thereby creating enormous out-of-balance positions and cost overruns. Servicing problems may precipitate a technical default, which in turn could lead to premature redemption or accelerated repayment of the security. A firm in the role of servicer also may incur collection costs on nonperforming assets that exceed servicing fee income.

RISK MANAGEMENT OF ASSET SECURITIZATIONS

A firm should address the risks arising from its securitization activities as part of its overall risk-management system, including

- establishing clear roles for its board of directors and senior management;
- adopting appropriate policies, procedures, and processes to manage the firm's risks;
- establishing a process for measuring and monitoring risks; and
- maintaining appropriate internal controls to verify the integrity of processes associated with these activities.

For more information, see SR-99-37, "Risk Management and Valuation of Retained Interests Arising from Securitization Activities." Firms with significant securitization activities are expected to have established more elaborate and formal approaches to manage the risks associated with these activities and should ensure that risk exposures resulting from these activities are fully incorporated into relevant management information system reports and risk-management reviews.

The Roles of Senior Management and the Board of Directors

A firm's board of directors is responsible for overseeing the development of, reviewing, approving, and periodically monitoring the firm's strategy and risk appetite.[2] As such, the board of directors should have an understanding of the firm's securitization activities and the associated risks. The board should approve significant policies relating to the firm's strategy and risk exposure arising from its securitization activities. The board also should hold senior management accountable for effectively implementing the firm's securitization strategy in a manner consistent with its risk appetite while maintaining an effective risk-management framework and system of internal controls.

2. For more information, see SR-21-3, "Supervisory Guidance on Board of Directors' Effectiveness," which generally applies to domestic bank holding companies and savings and loan holding companies with total consolidated assets of $100 billion or more.

Senior management is responsible for ensuring that the formality and sophistication of the techniques used to manage these risks are commensurate with the nature and volume of the firm's securitization activities. Senior management is responsible for ensuring that the risks arising from securitization activities are adequately managed on both a short-term and long-run basis. Management should ensure that adequate policies and procedures are in place for incorporating the risk of these activities into the firm's overall risk-management process.

Policies and Procedures

A firm's policies and procedures for asset securitization activities should ensure that the economic substance of the risk exposures generated by these activities is fully recognized and appropriately managed. In addition, firms involved in securitization activities should have appropriate policies, procedures, and controls for underwriting ABS; funding the possible return of revolving receivables (for example, credit card receivables and home-equity lines); and establishing limits on exposures to individual institutions, types of collateral, and geographic and industry concentrations.

To manage the risks associated with asset securitization activities appropriately, firms typically should—

- establish independent risk-management processes, including appropriate information systems, to monitor securitization-pool performance on an individual and aggregate transaction level;
- use conservative valuation assumptions and modeling methodologies to establish, evaluate, and adjust the carrying value of retained interests on a regular and timely basis;
- ensure staff in the audit or internal review functions periodically review data integrity, model algorithms, key underlying assumptions, and the appropriateness of the valuation and modeling process for any securitized assets retained by the institution, and report such findings to the board or an appropriate board committee;
- maintain accurate and timely risk-based capital calculations, including recognition and reporting of any recourse obligation resulting from a securitization activity;
- establish internal limits to govern the maximum amount of retained interests in any security as a percentage of total equity capital; and
- have a realistic liquidity plan in place in case of market disruptions.

Independent Risk-Management Function

Firms engaged in securitization activities should have an independent risk-management function commensurate with the complexity and volume of their securitization activity and their overall risk exposures. Considering a firm's securitization activities, the risk-management function should maintain appropriate policies and operating procedures, including clearly articulated risk limits. An effective asset-securitization policy generally—

- describes the maintenance of a consistently applied accounting methodology;
- explains the regulatory reporting requirements;
- covers valuation methodologies, including residual value assumptions, and formal procedures to approve changes to those assumptions;
- addresses management reporting process(es); and
- contains exposure limits and requirements for both individual- and aggregate-transaction monitoring.

The firm's risk-management function is responsible for monitoring origination, collection, and default-management practices. This includes regular evaluations of the quality of underwriting, soundness of the collateral valuation process, effectiveness of collection activities, ability of the default-management staff to resolve severely delinquent loans in a timely and efficient manner, and appropriateness of loss-recognition practices. Because the securitization of assets can result in current recognition of anticipated income, the risk-management function should monitor the types, volumes, and risks of assets being originated, transferred, and serviced. Senior management and the risk-management staff should be cognizant of any misaligned incentives among line managers to originate abnormally large volumes or higher-risk assets to meet income projections. Such misaligned incentives can lead to potential com-

promise of credit-underwriting standards, which may accelerate credit losses in future periods, impair the value of retained interests, or potentially lead to funding problems.

Risk Measurement and Monitoring

A firm's risk-management function should include systems to measure and monitor risks in a way that fully incorporates all risks involved in its securitization activities. The risk-management function should appropriately identify credit exposures from all securitization activities, and also should measure, quantify, and control those exposures on a fully consolidated basis. The economic substance of the credit exposures of securitization activities should be fully incorporated into the firm's efforts to quantify its credit risk, including efforts to establish more formal grading of credits to allow for statistical estimation of loss-probability distributions. Securitization activities should also be included in any aggregations of credit risk by borrower, industry, or economic sector.

A firm's information systems should identify and segregate those credit exposures arising from the firm's loan-sale and securitization activities. Such exposures include the sold portions of loan participations and syndications, exposures arising from the extension of credit-enhancement and liquidity facilities, the effects of any early-amortization event, and any investment(s) in ABS. Effective reports provide senior management with timely and sufficient information to monitor the firm's exposure limits and overall risk profile with respect to its securitization activities.

Stress Testing

The use of stress testing, including combinations of market events that could affect a firm's credit exposures and securitization activities, is another important element of risk management. Stress testing involves identifying possible events or changes in market behavior that could have unfavorable effects on the institution and assessing the firm's ability to withstand them. Stress testing should consider the probability of adverse events, including likely worst-case scenarios. An effective stress testing program is conducted by a firm on a consolidated basis and considers, for instance, the effect of higher-than-expected levels of delinquencies and defaults in the underlying asset pool. The firm should also consider the consequences of early-amortization events with respect to credit card securities, as these could raise concerns regarding the firm's capital adequacy and its liquidity and funding capabilities. Stress-test analyses should also include contingency plans for possible management actions in over a range of situations.

Internal Controls

One of management's most important responsibilities is establishing and maintaining an effective system of internal controls. A firm's internal controls should enforce the official lines of authority and the appropriate separation of duties established for managing the firm's risks. These internal controls should consider the type and level of risks, given the nature and scope of the firm's securitization activities. Moreover, these internal controls should ensure that financial reporting (in public financial statements and regulatory financial reports) is reliable.

Effective internal controls are essential to a firm's management of the risks associated with securitization. When properly designed and consistently enforced, a sound system of internal controls will help management safeguard the firm's resources; ensure that financial information and reports are reliable; and confirm that the firm is complying with contractual obligations, including any securitization covenants. Internal controls will also detect and reduce the possibility of significant errors and irregularities. Internal controls typically (1) limit authorities; (2) safeguard access to and use of records; (3) separate and rotate duties; and (4) ensure both regular and unscheduled reviews, including transaction testing.

Operational and managerial standards have been established for internal control and information systems.[3] A firm should maintain an appropriate system of internal controls based on the size, nature, scope, and the risk of the firm's activities.[4]

3. *See* 12 CFR 208, appendix D-1 (describing safety-and-soundness standards for state member banks).

4. Regulated financial institutions that are subject to the requirements of 12 CFR pt. 363 issued by the FDIC should include an assessment of the effectiveness of internal controls

Audit Function or Internal Review

Through its risk and audit committees, an effective board of directors assesses and supports the stature and independence of the firm's independent risk management and internal audit functions. The firm's audit staff or independent-review function should be competent and fully capable of reviewing the firm's securitization activities. The audit function should perform periodic reviews of securitization activities, including transaction testing and verification, and report all findings to the board or appropriate board committee. The audit function also may assist senior management in identifying and measuring risk related to securitization activities. Principal audit targets should include compliance with securitization policies, operating and accounting procedures, securitization covenants, and the accuracy of management information systems and regulatory reports. The audit function also should confirm that the firm's regulatory reporting process is designed and managed to facilitate timely and accurate reporting. Furthermore, when a third-party services the loans underlying the securitization, the auditors should perform an independent verification of the existence of the loans to ensure that balances reconcile to internal records.

Management Information Systems

Adequate reports on the performance of assets in the ABS from management information system (MIS) can help a firm appropriately manage the amount of economic capital to cover the various risks inherent in a securitization transaction. A firm's reporting and documentation methods should support the initial valuation of any retained interests in securitized assets and provide ongoing impairment analyses of these assets. In general, effective MIS reports address the following:

- *Securitization summaries for each ABS transaction.* The summary should include relevant transaction terms, such as collateral type, liquidity facilities, maturity, credit-enhancement and subordination features, financial covenants (termination events and spread-account capture triggers), any repurchase rights or obligations, and counterparty exposures. Management should distribute transaction summaries to appropriate personnel associated with securitization activities.
- *Performance reports by portfolio and specific product type.* Performance factors include gross portfolio yield, default rates and loss severity, delinquencies, prepayments, payments, and excess spread amounts. The reports should reflect the performance of assets, both on an individual-pool basis and across total managed assets. These reports should segregate specific products issued by the firm.
- *Historical (or vintage) analysis for each pool using monthly data.* Historical analysis helps management understand past performance trends and their implications for future default rates, prepayments, and delinquencies, and therefore valuation of any retained interests. Management can use these reports to compare historical performance trends with underwriting standards, including the use of a validated credit-scoring model, to ensure loan pricing is consistent with risk levels. Historical or trend analysis also helps in the comparison of deal performance at periodic intervals and helps validate retained-interest valuation assumptions.
- *Static-pool cash-collection analysis.* A static-pool cash-collection analysis involves (1) reviewing monthly cash receipts relative to the principal balance of the pool to determine the cash yield on the portfolio, (2) comparing the cash yield to the accrual yield, and (3) tracking monthly changes. Management should compare on a monthly basis the timing and amount of cash flows received from the securitization trust with those projected as part of the retained-interest valuation analysis. Some master-trust structures allow excess cash flow to be shared between series or pools. For revolving-asset trusts with this master-trust structure, management should perform a cash-collection analysis for each master-trust structure. These analyses are critical in assessing the actual performance of the portfolio in terms of default and prepayment rates. If cash receipts are less than those assumed in the original valuation of the retained interest, this analysis will provide a firm with an early warning of possible problems with collections or extension practices and impairment of the retained interest.

over their asset-securitization activities as part of management's report on the overall effectiveness of the system of internal controls over financial reporting. This assessment implicitly includes internal controls over financial information that the firm includes in its regulatory reporting.

- *Sensitivity analysis.* A sensitivity analysis measures a range of activities, such as the effect of changes in default rates, prepayment rates, payment rates, or discount rates, and assists management in establishing and validating the carrying value of the retained interest. Effective sensitivity analysis is performed at least quarterly. Analyses should consider potential adverse trends and determine "best," "probable," and "worst-case" scenarios for each event. Other relevant factors may include the effect of increased defaults on collection staff resources, the timing of cash flows, spread-account capture triggers, overcollateralization triggers, and early-amortization triggers. An increase in defaults can result in higher-than-expected costs and a delay in cash flows, thus decreasing the value of the retained interests. Management should periodically assess how changes in retained interests affect both the firm's earnings and its capital. Management should incorporate this analysis into their overall interest-rate-risk measurement system and include this analysis in information provided to the firm's board of directors or an appropriate board committee.
- *Statement of covenant compliance.* Ongoing compliance with deal-performance triggers as defined by the pooling and servicing agreements should be affirmed at least monthly. Performance triggers include early amortization, spread capture, changes to overcollateralization requirements, and events that could result in the firm being removed as servicer.

A firm must not include confidential supervisory information related to supervisory actions or thresholds in any covenants included in documents related to a securitization transaction.[5] Examples of such supervisory actions include a downgrade in a bank's CAMELS rating, an enforcement action, or a downgrade in a bank's prompt-corrective-action capital category. Further, covenants that provide for the early termination of the transaction or compel the transfer of servicing due, directly or indirectly, to the occurrence of a supervisory action or event will be criticized, under appropriate circumstances, as an unsafe and unsound banking practice.[6] Any early amortization or transfer of servicing triggered by such events can create or exacerbate liquidity and earnings problems for a firm, which in turn may lead to further deterioration in its financial condition.

CAPITAL ADEQUACY

The Federal Reserve's Regulation Q (12 CFR pt. 217) establishes a capital framework that considers the credit risk of exposures that involve the tranching of credit risk of one or more underlying securitization exposures. Regulation Q establishes risk weights for securitization exposures that are retained on- or off-balance sheet. Regulation Q defines a securitization exposure as an on- or off-balance-sheet credit exposure (including credit-enhancing representations and warranties) that arises from a traditional or synthetic securitization (including a resecuritization), or an exposure that directly or indirectly references such a securitization exposure.

Common examples of securitization exposures include private-label CMOs, trust-preferred collateralized debt obligations, and ABS, provided there is tranching of credit risk. In general, supervised institutions subject to Regulation Q's requirements calculate the risk weight of securitization exposures using methodologies prescribed in the rule, such as the gross-up approach or the Simplified Supervisory Formula Approach. The methodology must be applied consistently across all securitization exposures, except in certain cases.

For more information, see this manual's section entitled "Assessment of Capital Adequacy."

ACCOUNTING AND REPORTING

Sale or Borrowing Treatment

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

5. For more information on the treatment of confidential supervisory information, see 12 U.S.C. 1817(a) and 1831m, as well as 12 CFR 261 subpart C.

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

transfer should be treated as a sale of the assets or as a collateralized borrowing (meaning a financing transaction secured by assets).

When a loan is acquired (through origination or purchase) with the intent or expectation that it may or will be sold at some indefinite date in the future, the loan should be reported as held for sale or held for investment, based on consideration of all the facts and circumstances, in accordance with generally accepted accounting principles (GAAP) and related supervisory guidance. In addition, a loan acquired and held for securitization purposes should be reported as a loan held for sale, provided the securitization transaction will be accounted for as a sale under Accounting Standards Codification (ASC) Topic 860, Transfers and Servicing. Notwithstanding the above, banks may classify loans as trading assets if the bank applies fair value accounting, with changes in fair value reported in current earnings, and manages these assets and liabilities as trading assets, subject to the controls and applicable regulatory guidance related to trading activities. For example, a bank generally would not classify a loan that meets these criteria as a trading asset unless the bank holds the loan for one of the following purposes: (a) to facilitate market making activities, including such activities as accumulating loans for sale or securitization; (b) to benefit from actual or expected price movements; or (c) to lock in arbitrage profits.

Institutions that file the Report of Condition and Income (Call Report) and are involved in securitization activities should pay particular attention to the following schedules on the Call Report: Schedule RC-F: Other Assets; Schedule RC-L: Off Balance Sheet Items; and Schedule RC-R: Regulatory Capital.

Valuation and Modeling Processes for Retained Interests

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

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

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

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

To determine the value of the retained interest at inception, and to make appropriate adjustments going forward, the institution should implement a reasonable modeling process to comply with ASC Topic 860. Management is expected to employ reasonable and conservative valuation assumptions and projections and to maintain verifiable objective documentation of the fair value of the retained interest. Senior management is responsible for ensuring that the valuation model accurately reflects the cash flows according to the terms of the securitization's structure. For example, the model should account for any cash collateral or overcollater-

alization triggers, trust fees, and insurance payments, as appropriate. Management is accountable for ensuring that the model builder(s) possess the necessary expertise and technical proficiency to perform the modeling process. Senior management should ensure that internal controls are in place to provide for the ongoing integrity of MIS associated with securitization activities.

As part of the modeling process, the risk-management function should ensure that periodic validations are performed to reduce vulnerability to model risk. Validation of the model includes testing the internal logic, ensuring empirical support for the model assumptions, and back-testing the models using actual cash flows on a pool-by-pool basis. The validation process should be documented to support conclusions. Senior management should ensure that the validation process is independent from line management and from the modeling process. The audit scope should include procedures to ensure that the modeling process and validation mechanisms are both appropriate for the institution's circumstances and executed consistently with its asset-securitization policy.

Use of Outside Parties

Third parties are often engaged to provide professional guidance and support regarding a firm's securitization activities and transactions as well as valuation of retained interests. The use of outside resources does not relieve a board of directors of its oversight responsibility, nor does it relieve senior management of its responsibilities to provide supervision, monitoring, and oversight of securitization activities, particularly management of the risks associated with retained interests. Management is expected to have the experience, knowledge, and abilities to discharge its duties; to understand the nature and extent of the risks presented by retained interests; and to have the policies and procedures necessary to implement an effective risk-management system to control such risks. Management should have an understanding of the valuation techniques used to determine the value of the firm's interest in a securitization, including the basis and reasonableness of underlying assumptions and projections.

Market Discipline and Disclosures

Transparency through public disclosure is crucial to effective market discipline and can reinforce supervisory expectations for a firm's risk management. Timely and adequate information on a firm's asset-securitization activities should be disclosed. The information in the firm's public disclosures should be comprehensive; however, the amount of disclosure that is appropriate will depend on the volume of securitizations and the complexity of the firm's securitization activities. Well informed investors, depositors, creditors, and other counterparties can provide a firm with strong incentives for maintaining sound risk-management systems and internal controls.

Adequate disclosure allows market participants to understand a firm's financial condition and apply market discipline, thus creating incentives to reduce inappropriate risk-taking or to address inadequate risk-management practices. Examples of sound disclosures include—

- accounting policies for measuring retained interests, including a discussion of the implications of key assumptions on the recorded value of the firm's interest in the securitization(s);
- the process and methodology used to adjust the value of retained interests for changes in key assumptions;
- quantitative and qualitative risk characteristics of the underlying securitized assets;
- the role of retained interests as credit enhancements to special-purpose entities and other securitization vehicles, including a discussion of techniques used for measuring credit risk; and
- sensitivity analyses conducted by the firm to understand the effect of changes in key assumptions on the fair value of retained interests.

SUPERVISORY CONSIDERATIONS

Examiners are expected to exercise judgment in determining which examination procedures are appropriate for assessing the securitization activities of an individual bank. The scope of each review will largely depend on the size and complexity of a bank's securitization activities as well as the ability of the bank to manage the

risks associated with these activities appropriately. The Securitization Examination Documentation (ED) module provides more detailed examination procedures for examination staff. The Securitization ED module primarily applies to examinations of banks that use securitizations to transfer financial assets off their balance sheets. The ED Module also applies to the review of banks that originate or purchase financial assets for securitization; retain beneficial interests in securitized assets; or provide liquidity or credit enhancements.

As previously noted, securitization activities have the potential to increase the overall risk profile of the bank if the activities are not carried out prudently. Banks that engage in securitization activities encounter various risks, such as credit, concentration, interest-rate, operational, and liquidity risks. The nature of a bank's securitization activities and the bank's ability to manage those activities will influence how examiners assign supervisory ratings, particularly a bank's CAMELS component or composite ratings.

For example, examiners should determine whether the bank has sufficient capital in relation to risks arising from securitization activities. If, in the examiner's judgment, a bank's capital level is not sufficient to provide protection against potential losses from securitization activities, this deficiency should be reflected in the bank's CAMELS rating and discussed with bank management. In such situations, examiners would expect that the bank would develop and implement a plan for strengthening its overall capital adequacy to levels deemed appropriate given its risk exposure.

Asset securitization activities can adversely influence how examiners rate a bank's asset quality in several ways. A bank that originates abnormally large volumes or higher-risk assets to sustain ongoing income needs potentially may compromise its credit-underwriting standards. The result could be an acceleration of credit losses in future periods. Further, a bank could be exposed to concentration risk if its securitized assets contain excessive exposures to an industry or region.

In terms of the assessment of liquidity, one factor examiners should consider is a bank's ability to securitize and sell certain pools of assets.[7] While securitization can be an effective funding method for some banks, there are several risks.[8] For instance, banks that originate or purchase loans for asset securitization programs may face heightened liquidity risk due to unexpected funding needs associated with an early amortization event or disruption of warehouse funding. Furthermore, the bank's overall cash flow might be dependent on the residual cash flows from the performance of the underlying assets. If the performance of the underlying assets is worse than projected, the bank's overall cash flow will be less than anticipated, which would adversely affect the bank's liquidity. Examiners should determine whether a bank has reviewed the projected cash flow from the underlying assets to ensure that principal and interest payments will be timely and will be sufficient to cover costs even under adverse scenarios.

Securitization activities could affect the way examiners assess the sensitivity to market risk component rating of the CAMELS rating system. Examiners should assess whether banks engaged in underwriting or market-making activities have implemented adequate hedging or other risk-management policies to limit exposure to adverse price movements. For instance, banks should appropriately manage changes in default rates, prepayment rates, payment rates, and discount rates when establishing and validating the carrying value of any retained interest(s). Examiners should review a bank's analysis as well as the volatility associated with retained interests when assessing a bank's sensitivity to market risk component rating.[9]

Further, the ability of banks to appropriately manage and monitor the risks associated with securitization activities will influence examiners' assessment of a bank's management rating. For example, if bank management conducts securitization activities in a manner that is inconsistent with the bank's strategic and financial objectives, such conduct may adversely affect the bank's management rating. The management rating could also be adversely affected if a bank exhibits internal control failures or is not appropriately responsive to findings arising from internal audits, independent reviews, or previous supervisory assessments of the bank's securitization function.

7. SR-96-38, "Uniform Financial Institutions Rating System."

8. SR-10-6, "Interagency Policy Statement on Funding and Liquidity Risk Management."

9. SR-96-13, "Joint Agency Policy Statement on Interest-Rate Risk," advises that examiners may direct institutions with a high level of exposure to interest-rate risk relative to capital to take corrective action.

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:

- Securitization

This section sets forth the Interagency Statement on Sound Practices Concerning Elevated-Risk Complex Structured Finance Activities, issued January 11, 2007.[1] The supervisory guidance addresses risk-management principles that should assist institutions to identify, evaluate, and manage the heightened legal and reputational risks that may arise from their involvement in complex structured finance transactions (CSFTs). The guidance is focused on sound practices related to CSFTs that may create heightened legal or reputational risks to the institution and are defined as ''elevated-risk CSFTs.'' Such transactions are typically conducted by a limited number of large financial institutions.[2] (See SR-07-05.)

INTERAGENCY STATEMENT ON SOUND PRACTICES CONCERNING ELEVATED-RISK COMPLEX STRUCTURED FINANCE ACTIVITIES

Financial markets have grown rapidly over the past decade, and innovations in financial instruments have facilitated the structuring of cash flows and allocation of risk among creditors, borrowers, and investors in more efficient ways. Financial derivatives for market and credit risk, asset-backed securities with customized cash-flow features, specialized financial conduits that manage pools of assets, and other types of structured finance transactions serve important business purposes, such as diversifying risks, allocating cash flows, and reducing cost of capital. As a result, structured finance transactions have become an essential part of U.S. and international capital markets. Financial institutions have played and continue to play an active and important role in the development of structured finance products and markets, including the market for the more complex variations of structured finance products.

When a financial institution[3] participates in a CSFT, it bears the usual market, credit, and operational risks associated with the transaction. In some circumstances, a financial institution also may face heightened legal or reputational risks due to its involvement in a CSFT. For example, in some circumstances, a financial institution may face heightened legal or reputational risk if a customer's regulatory, tax, or accounting treatment for a CSFT, or disclosures to investors concerning the CSFT in the customer's public filings or financial statements, do not comply with applicable laws, regulations, or accounting principles. Indeed, in some instances, CSFTs have been used to misrepresent a customer's financial condition to investors, regulatory authorities, and others. In these situations, investors have been harmed and financial institutions have incurred significant legal and reputational exposure. In addition to legal risk, reputational risk poses a significant threat to financial institutions because the nature of their business requires them to maintain the confidence of customers, creditors, and the general marketplace.

The agencies[4] have long expected financial institutions to develop and maintain robust control infrastructures that enable them to identify, evaluate, and address the risks associated with their business activities. Financial institutions also must conduct their activities in accordance with applicable statutes and regulations.

Scope and Purpose of Statement

The agencies issued this statement to describe the types of risk-management principles they believe may help a financial institution to identify CSFTs that may pose heightened legal or reputational risks to the institution and to evalu-

1. See 72 *Fed. Reg.* 1372, January 11, 2007.

2. The statement will not affect or apply to the vast majority of financial institutions, including most small institutions.

3. As used in this statement, the term *financial institution* or *institution* refers to state member banks and bank holding companies (other than foreign banking organizations) in the case of the Board of Governors of the Federal Reserve System (FRB); to national banks in the case of the Office of the Comptroller of the Currency (OCC); to federal and state savings associations and savings and loan holding companies in the case of the Office of Thrift Supervision (OTS); to state nonmember banks in the case of the Federal Deposit Insurance Corporation (FDIC); and to registered broker-dealers and investment advisers in the case of the Securities and Exchange Commission (SEC). The U.S. branches and agencies of foreign banks supervised by the FRB, the OCC, and the FDIC also are considered to be financial institutions for purposes of this statement.

4. The federal banking agencies (the FRB, the OCC, the FDIC, and the OTS) and the SEC.

ate, manage, and address these risks within the institution's internal control framework.

Structured finance transactions encompass a broad array of products with varying levels of complexity. Most structured finance transactions, such as standard public mortgage-backed securities transactions, public securitizations of retail credit cards, asset-backed commercial paper conduit transactions, and hedging-type transactions involving ''plain vanilla'' derivatives and collateralized loan obligations, are familiar to participants in the financial markets, and these vehicles have a well-established track record. These transactions typically would not be considered CSFTs for the purpose of this statement.

Because this statement focuses on sound practices related to CSFTs that may create heightened legal or reputational risks—transactions that typically are conducted by a limited number of large financial institutions—it will not affect or apply to the vast majority of financial institutions, including most small institutions. As in all cases, a financial institution should tailor its internal controls so that they are appropriate in light of the nature, scope, complexity, and risks of its activities. Thus, for example, an institution that is actively involved in structuring and offering CSFTs that may create heightened legal or reputational risk for the institution should have a more formalized and detailed control framework than an institution that participates in these types of transactions less frequently. The internal controls and procedures discussed in this statement are not all-inclusive, and, in appropriate circumstances, an institution may find that other controls, policies, or procedures are appropriate in light of its particular CSFT activities.

Because many of the core elements of an effective control infrastructure are the same regardless of the business line involved, this statement draws heavily on controls and procedures that the agencies previously have found to be effective in assisting a financial institution to manage and control risks and identifies ways in which these controls and procedures can be effectively applied to elevated-risk CSFTs. Although this statement highlights some of the most significant risks associated with elevated-risk CSFTs, it is not intended to present a full exposition of all risks associated with these transactions. Financial institutions are encouraged to refer to other supervisory guidance prepared by the agencies for further information concerning market, credit, operational, legal, and reputational risks as well as internal audit and other appropriate internal controls.

This statement does not create any private rights of action and does not alter or expand the legal duties and obligations that a financial institution may have to a customer, its shareholders, or other third parties under applicable law. At the same time, adherence to the principles discussed in this statement would not necessarily insulate a financial institution from regulatory action or any liability the institution may have to third parties under applicable law.

Identification and Review of Elevated-Risk CSFTs

A financial institution that engages in CSFTs should maintain a set of formal, written, firmwide policies and procedures that are designed to allow the institution to identify, evaluate, assess, document, and control the full range of credit, market, operational, legal, and reputational risks associated with these transactions. These policies may be developed specifically for CSFTs, or included in the set of broader policies governing the institution generally. A financial institution operating in foreign jurisdictions may tailor its policies and procedures as appropriate to account for, and comply with, the applicable laws, regulations, and standards of those jurisdictions.[5]

A financial institution's policies and procedures should establish a clear framework for the review and approval of individual CSFTs. These policies and procedures should set forth the responsibilities of the personnel involved in the origination, structuring, trading, review, approval, documentation, verification, and execution of CSFTs. Financial institutions may find it helpful to incorporate the review of new CSFTs into their existing new-product policies. In this regard, a financial institution should define what constitutes a ''new'' complex structured finance product and establish a control process for the approval of such new products. In determining

5. In the case of U.S. branches and agencies of foreign banks, these policies, including management, review, and approval requirements, should be coordinated with the foreign bank's group-wide policies developed in accordance with the rules of the foreign bank's home-country supervisor and should be consistent with the foreign bank's overall corporate and management structure as well as its framework for risk management and internal controls.

whether a CSFT is new, a financial institution may consider a variety of factors, including whether it contains structural or pricing variations from existing products; whether the product is targeted at a new class of customers; whether it is designed to address a new need of customers; whether it raises significant new legal, compliance, or regulatory issues; and whether it or the manner in which it would be offered would materially deviate from standard market practices. An institution's policies should require new complex structured finance products to receive the approval of all relevant control areas that are independent of the profit center before the product is offered to customers.

Identifying Elevated-Risk CSFTs

As part of its transaction and new-product approval controls, a financial institution should establish and maintain policies, procedures, and systems to identify elevated-risk CSFTs. Because of the potential risks they present to the institution, transactions or new products identified as elevated-risk CSFTs should be subject to heightened reviews during the institution's transaction or new-product approval processes. Examples of transactions that an institution may determine warrant this additional scrutiny are those that (either individually or collectively) appear to the institution during the ordinary course of its transaction approval or new-product approval process to—

- lack economic substance or business purpose;
- be designed or used primarily for questionable accounting, regulatory, or tax objectives, particularly when the transactions are executed at year-end or at the end of a reporting period for the customer;
- raise concerns that the client will report or disclose the transaction in its public filings or financial statements in a manner that is materially misleading or inconsistent with the substance of the transaction or applicable regulatory or accounting requirements;
- involve circular transfers of risk (either between the financial institution and the customer or between the customer and other related parties) that lack economic substance or business purpose;
- involve oral or undocumented agreements that, when taken into account, would have a material impact on the regulatory, tax, or accounting treatment of the related transaction, or the client's disclosure obligations;[6]
- have material economic terms that are inconsistent with market norms (for example, deep "in the money" options or historic rate rollovers); or
- provide the financial institution with compensation that appears substantially disproportionate to the services provided or investment made by the financial institution or to the credit, market, or operational risk assumed by the institution.

The examples listed previously are provided for illustrative purposes only, and the policies and procedures established by financial institutions may differ in how they seek to identify elevated-risk CSFTs. The goal of each institution's policies and procedures, however, should remain the same: to identify those CSFTs that warrant additional scrutiny in the transaction or new-product approval process due to concerns regarding legal or reputational risks.

Financial institutions that structure or market, act as an advisor to a customer regarding, or otherwise play a substantial role in a transaction may have more information concerning the customer's business purpose for the transaction and any special accounting, tax, or financial disclosure issues raised by the transaction than institutions that play a more limited role. Thus, the ability of a financial institution to identify the risks associated with an elevated-risk CSFT may differ depending on its role.

Due Diligence, Approval, and Documentation Process for Elevated-Risk CSFTs

Having developed a process to identify elevated-risk CSFTs, a financial institution should implement policies and procedures to conduct a heightened level of due diligence for these transactions. The financial institution should design these policies and procedures to allow personnel at an appropriate level to understand and evaluate the potential legal or reputational risks presented by

6. This item is not intended to include traditional, nonbinding "comfort" letters or assurances provided to financial institutions in the loan process where, for example, the parent of a loan customer states that the customer (i.e., the parent's subsidiary) is an integral and important part of the parent's operations.

the transaction to the institution and to manage and address any heightened legal or reputational risks ultimately found to exist with the transaction.

Due diligence. If a CSFT is identified as an elevated-risk CSFT, the institution should carefully evaluate and take appropriate steps to address the risks presented by the transaction, with a particular focus on those issues identified as potentially creating heightened levels of legal or reputational risk for the institution. In general, a financial institution should conduct the level and amount of due diligence for an elevated-risk CSFT that is commensurate with the level of risks identified. A financial institution that structures or markets an elevated-risk CSFT to a customer, or that acts as an advisor to a customer or investors concerning an elevated-risk CSFT, may have additional responsibilities under the federal securities laws, the Internal Revenue Code, state fiduciary laws, or other laws or regulations and, thus, may have greater legal- and reputational-risk exposure with respect to an elevated-risk CSFT than a financial institution that acts only as a counterparty for the transaction. Accordingly, a financial institution may need to exercise a higher degree of care in conducting its due diligence when the institution structures or markets an elevated-risk CSFT or acts as an advisor concerning such a transaction than when the institution plays a more limited role in the transaction.

To appropriately understand and evaluate the potential legal and reputational risks associated with an elevated-risk CSFT that a financial institution has identified, the institution may find it useful or necessary to obtain additional information from the customer or to obtain specialized advice from qualified in-house or outside accounting, tax, legal, or other professionals. As with any transaction, an institution should obtain satisfactory responses to its material questions and concerns prior to consummation of a transaction.[7]

In conducting its due diligence for an elevated-risk CSFT, a financial institution should independently analyze the potential risks to the institution from both the transaction and the institution's overall relationship with the customer. Institutions should not conclude that a transaction identified as being an elevated-risk CSFT involves minimal or manageable risks solely because another financial institution will participate in the transaction or because of the size or sophistication of the customer or counterparty. Moreover, a financial institution should carefully consider whether it would be appropriate to rely on opinions or analyses prepared by or for the customer concerning any significant accounting, tax, or legal issues associated with an elevated-risk CSFT.

Approval process. A financial institution's policies and procedures should provide that CSFTs identified as having elevated legal or reputational risk are reviewed and approved by appropriate levels of control and management personnel. The designated approval process for such CSFTs should include representatives from the relevant business line(s) and/or client management, as well as from appropriate control areas that are independent of the business line(s) involved in the transaction. The personnel responsible for approving an elevated-risk CSFT on behalf of a financial institution should have sufficient experience, training, and stature within the organization to evaluate the legal and reputational risks, as well as the credit, market, and operational risks to the institution.

The institution's control framework should have procedures to deliver the necessary or appropriate information to the personnel responsible for reviewing or approving an elevated-risk CSFT to allow them to properly perform their duties. Such information may include, for example, the material terms of the transaction, a summary of the institution's relationship with the customer, and a discussion of the significant legal, reputational, credit, market, and operational risks presented by the transaction.

Some institutions have established a senior management committee that is designed to involve experienced business executives and senior representatives from all of the relevant control functions within the financial institution (including such groups as independent risk management, tax, accounting, policy, legal, compliance, and financial control) in the oversight and approval of those elevated-risk CSFTs that are identified by the institution's personnel as requiring senior management review and approval due to the potential risks associated with the transactions. While this type of management committee may not be appropriate for all financial institutions, a financial institution should establish processes that assist the institution in con-

7. Of course, financial institutions also should ensure that their own accounting for transactions complies with applicable accounting standards, consistently applied.

sistently managing the review and approval of elevated-risk CSFTs on a firm-wide basis.[8]

If, after evaluating an elevated-risk CSFT, the financial institution determines that its participation in the CSFT would create significant legal or reputational risks for the institution, the institution should take appropriate steps to address those risks. Such actions may include declining to participate in the transaction, or conditioning its participation upon the receipt of representations or assurances from the customer that reasonably address the heightened legal or reputational risks presented by the transaction. Any representations or assurances provided by a customer should be obtained before a transaction is executed and be received from, or approved by, an appropriate level of the customer's management. A financial institution should decline to participate in an elevated-risk CSFT if, after conducting appropriate due diligence and taking appropriate steps to address the risks from the transaction, the institution determines that the transaction presents unacceptable risk to the institution or would result in a violation of applicable laws, regulations, or accounting principles.

Documentation. The documentation that financial institutions use to support CSFTs is often highly customized for individual transactions and negotiated with the customer. Careful generation, collection, and retention of documents associated with elevated-risk CSFTs are important control mechanisms that may help an institution monitor and manage the legal, reputational, operational, market, and credit risks associated with the transactions. In addition, sound documentation practices may help reduce unwarranted exposure to the financial institution's reputation.

A financial institution should create and collect sufficient documentation to allow the institution to—

- document the material terms of the transaction;
- enforce the material obligations of the counterparties;
- confirm that the institution has provided the customer any disclosures concerning the transaction that the institution is otherwise required to provide; and
- verify that the institution's policies and procedures are being followed and allow the internal audit function to monitor compliance with those policies and procedures.

When an institution's policies and procedures require an elevated-risk CSFT to be submitted for approval to senior management, the institution should maintain the transaction-related documentation provided to senior management as well as other documentation, such as minutes of the relevant senior management committee, that reflect senior management's approval (or disapproval) of the transaction, any conditions imposed by senior management, and the factors considered in taking such action. The institution should retain documents created for elevated-risk CSFTs in accordance with its record retention policies and procedures as well as applicable statutes and regulations.

Other Risk-Management Principles for Elevated-Risk CSFTs

General business ethics. The board and senior management of a financial institution also should establish a "tone at the top" through both actions and formalized policies that sends a strong message throughout the financial institution about the importance of compliance with the law and overall good business ethics. The board and senior management should strive to create a firm-wide corporate culture that is sensitive to ethical or legal issues as well as the potential risks to the financial institution that may arise from unethical or illegal behavior. This kind of culture coupled with appropriate procedures should reinforce business-line ownership of risk identification and encourage personnel to move ethical or legal concerns regarding elevated-risk CSFTs to appropriate levels of management. In appropriate circumstances, financial institutions may also need to consider implementing mechanisms to protect personnel by permitting the confidential disclosure of concerns.[9] As in other areas of financial institution management, compensation and incentive plans

8. The control processes that a financial institution establishes for CSFTs should take account of, and be consistent with, any informational barriers established by the institution to manage potential conflicts of interest, insider trading, or other concerns.

9. The agencies note that the Sarbanes-Oxley Act of 2002 requires companies listed on a national securities exchange or inter-dealer quotation system of a national securities association to establish procedures that enable employees to submit concerns regarding questionable accounting or auditing mat-

should be structured, in the context of elevated-risk CSFTs, so that they provide personnel with appropriate incentives to have due regard for the legal-, ethical-, and reputational-risk interests of the institution.

Reporting. A financial institution's policies and procedures should provide for the appropriate levels of management and the board of directors to receive sufficient information and reports concerning the institution's elevated-risk CSFTs to perform their oversight functions.

Monitoring compliance with internal policies and procedures. The events of recent years evidence the need for an effective oversight and review program for elevated-risk CSFTs. A financial institution's program should provide for periodic independent reviews of its CSFT activities to verify and monitor that its policies and controls relating to elevated-risk CSFTs are being implemented effectively and that elevated-risk CSFTs are accurately identified and have received proper approvals. These independent reviews should be performed by appropriately qualified audit, compliance, or other personnel in a manner consistent with the institution's overall framework for compliance monitoring, which should include consideration of issues such as the independence of reviewing personnel from the business line. Such monitoring may include more-frequent assessments of the risk arising from elevated-risk CSFTs, both individually and within the context of the overall customer relationship, and the results of this monitoring should be provided to an appropriate level of management in the financial institution.

Audit. The internal audit department of any financial institution is integral to its defense against fraud, unauthorized risk taking, and damage to the financial institution's reputation. The internal audit department of a financial institution should regularly audit the financial institution's adherence to its own control procedures relating to elevated-risk CSFTs, and further assess the adequacy of its policies and procedures related to elevated-risk CSFTs. Internal audit should periodically validate that business lines and individual employees are complying with the financial institution's standards for elevated-risk CSFTs and appropriately identifying any exceptions. This validation should include transaction testing for elevated-risk CSFTs.

Training. An institution should identify relevant personnel who may need specialized training regarding CSFTs to be able to effectively perform their oversight and review responsibilities. Appropriate training on the financial institution's policies and procedures for handling elevated-risk CSFTs is critical. Financial institution personnel involved in CSFTs should be familiar with the institution's policies and procedures concerning elevated-risk CSFTs, including the processes established by the institution for identification and approval of elevated-risk CSFTs and new complex structured finance products and for the elevation of concerns regarding transactions or products to appropriate levels of management. Financial institution personnel involved in CSFTs should be trained to identify and properly handle elevated-risk CSFTs that may result in a violation of law.

CONCLUSION

Structured finance products have become an essential and important part of the U.S. and international capital markets, and financial institutions have played an important role in the development of structured finance markets. In some instances, however, CSFTs have been used to misrepresent a customer's financial condition to investors and others, and financial institutions involved in these transactions have sustained significant legal and reputational harm. In light of the potential legal and reputational risks associated with CSFTs, a financial institution should have effective risk-management and internal control systems that are designed to allow the institution to identify elevated-risk CSFTs; to evaluate, manage, and address the risks arising from such transactions; and to conduct those activities in compliance with applicable law.

ters on a confidential, anonymous basis. (See 15 USC 78j-1(m).)

Bank management is responsible for controlling risk at a level deemed acceptable for the organization. An effective risk-management program begins with the identification of exposures that could disrupt the timely and accurate delivery of business services or result in unexpected financial claims on bank resources. Risk management also involves the implementation of cost-effective controls and the shifting, transfer, or assignment of risk to third parties through insurance coverage or other risk-transfer techniques. Although the design and sophistication of risk-management procedures varies from bank to bank, each institution's decision-making process should effectively identify; control; and, when or where appropriate, result in some transfer of risk. The risk-assessment program should be conducted annually to establish whether potential service disruptions and estimated risk-related financial costs and losses can be contained at levels deemed acceptable to bank management and the board of directors. Note that insurance can provide a bank with the resources to restore business operations and financial stability only *after* an unanticipated event has occurred, but a bank's own risk-management controls can prevent and minimize losses before they occur.

RISK-MANAGEMENT PROGRAM

A sound operational risk-management program requires the annual review of all existing business operations and a risk assessment of all proposed services. Identified risks should be analyzed to estimate their potential and probable levels of loss exposure. While the historical loss experience of the bank and other service providers may be helpful in quantifying loss exposure, technological and societal changes may result in exposure levels that differ from historical experience. Nevertheless, current exposure estimates should be derived from the bank's historical loss experience and augmented with industry experience. In addition, the bank's insurance broker or agent should be a source of advice.

Management must decide the most appropriate method for addressing a particular risk. Although many factors influence this decision, the purpose of risk management is to minimize the probability of losses and the net costs associated with them. In that context, cost is broadly defined to include—

- the direct and consequential cost of loss-prevention measures (controls), plus
- insurance premiums, plus
- losses sustained, including the consequential effects and expenses to reduce such losses, minus
- recoveries from third parties and indemnities from insurers on account of such losses, plus
- pertinent administrative costs.

Bank risks with potentially high or even catastrophic financial consequences should be eliminated or substantially mitigated whenever possible, even when the risk's frequency of occurrence is low. These risks can be eliminated by discontinuing operations where appropriate or by assigning the risk exposure to other parties using third-party service providers. When the exposure cannot be shifted to other parties or otherwise mitigated, the bank must protect itself with appropriate levels of insurance. Certain loss exposures may be deemed reasonable because their probability of frequency and severity of loss are low, the level of expected financial loss or service disruption is minimal, or the costs associated with the recovery of assets and restoration of services are low.

Bank management may decide to reduce insurance premiums and claims-processing costs by self-insuring for various types of losses, setting higher deductible levels, lowering the coverage limits for insurance purchased, and narrowing coverage terms and conditions. A financial organization's primary defenses against loss are adequate internal controls and procedures, which insurance is intended to complement, not replace. Thus, an overall appraisal of the organization's control environment is a significant consideration in determining the adequacy of the insurance program. To the extent that controls are lacking, the need for additional insurance coverage increases. These determinations should be based on the results of the risk assessment and be consistent with the limits established by the board of directors. Insurance decisions may also be influenced by the insurance broker's advice regarding current insurance market and premium trends.

Following September 2001, insurance companies reevaluated their position on providing coverage for acts of terrorism. As a result, terrorism coverage has become expensive or unavailable. The bank's "schedule of insurance" should note which policies contain exclusions, sublimits, or large deductibles for losses incurred as a result of terrorism.

When selecting insurance carriers, banks should consider the financial strength and claims-paying capacity of the insurance underwriter, as well as the robustness or strength of the supervisory regime to which the insurer is subject. This procedure is important for all significant policy-coverage lines. Rating agencies typically consider a number of insurers vulnerable, and some underwriters may have large environmental exposures but capped equity resources. Many large commercial enterprises acquire insurance coverage from foreign companies or from subsidiaries of U.S. insurers domiciled in the Caribbean or other countries. The quality of insurance supervision in many foreign countries may not meet the standards expected in the United States.

TYPES OF RISKS

Business risks generally fall into three categories: (1) physical property damage, (2) liability resulting from product failure or unintended employee performance, and (3) loss of key personnel. Common property risks are fires or natural disasters such as storms and earthquakes, but acts of violence or terrorism can also be included in this category. Risk-management programs for property damage should consider not only the protection and replacement of the physical plant, but also the effects of business interruptions, loss of business assets, and reconstruction of records.

Insurance programs increasingly cover the consequences of the second category, product failure or unintended employee performance. These risks include the injury or death of employees, customers, and others; official misconduct; and individual and class-action lawsuits alleging mistreatment or the violation of laws or regulations. All aspects of a bank's operation are susceptible to liability risks. While property-loss levels can be estimated with relative confidence, jury awards for personal injury or product liability, and the related litigation costs, often exceed expectations. In addition, it can be difficult to identify potential sources of liability exposure.

The third category, personnel risk, concerns those exposures associated with the loss of key personnel through death, disability, retirement, or resignation, as well as threats to all employees and third parties arising out of crimes such as armed robbery and extortion. The consequences of personnel loss are often more pronounced in small and medium-sized banks that do not have the financial resources to support a broad level of management.

INSURANCE PROGRAM

Program Objectives

A bank's insurance program should match the objectives of its management, the director-approved risk guidelines, and its individual risk profile. Insurance is primarily the transfer of the financial effect of losses and should be considered as only a part of the broader risk-management process. In that sense, it is imperative that management understands the costs and benefits of the bank's insurance program.

Due to the fluid nature of the insurance market and insurance products, there is no standard program or contract structure. Rather, many different insurance policies, coverages, endorsements, limits, deductibles, and payment plans fit together to form an insurance program. Based on the size and scope of a bank's operations, broader or narrower coverage, higher or lower limits, and separate policies may be purchased. Insurance programs should be customized to the risks that each bank faces. If a bank is particularly susceptible to a specific risk, purchasing additional insurance for that risk may be prudent.

A policy's deductible size and coverages, and the limits purchased, determine how much risk the bank has retained. Likewise, the payment plan of an insurance policy greatly influences the amount of risk transferred. An insurance policy alone does not represent significant risk transfer if the payment plan includes reimbursement to the insurance company for all losses, usually subject to a maximum. These reimbursement, loss-sensitive, or retrospectively rated plans can be viewed more as a risk-financing

tool than as risk transfer. Management should understand and quantify the total "all-in" cost of these plans, as well as how these costs correspond with the risk guidelines approved by the directors.

Common Insurance-Policy Components and Concepts

There is a difference between "policy" and "coverage," but the two terms are often used interchangeably. The term "policy" usually refers to the actual insurance contract, while the term "coverage" refers to the types of risks to which the policy is designed to respond. For example, a directors' and officers' policy may include employment-practices liability (EPL) coverage. However, the bank may also purchase a separate EPL policy

An "endorsement" is a modification to a policy. Endorsements can be either a simple change in wording from the original contract or a more complex addition or deletion of a coverage section. To expand on the example above, EPL coverage is often endorsed onto a directors' and officers' policy. When an endorsement adds a coverage to a policy, it is often called a "rider."

The "limit of insurance" is the dollar amount of insurance protection purchased. Each policy has a different limit, and some may have separate limits for separate coverages provided under the same policy. Policies usually include a "per-occurrence" and an "aggregate" limit. The per-occurrence limit is the most the insurer will pay under the policy for any one insured event, while the policy aggregate is the most the insurer will pay in total, regardless of the number and size of insurable events.

"Deductibles" and "self-insured retentions (SIRs)" are the dollar amounts the bank must contribute to the loss before insurance applies.[1] They are effectively the same concept, with the difference being a deductible reduces the limits of insurance while a SIR does not. A deductible is included within or as part of the limits. A SIR is outside or in addition to the provided limits. For example, a $5 million policy limit with a $1 million deductible consists of $4 million of protection and the $1 million deductible. A $5 million policy limit with a $1 million SIR provides $5 million in protection after the $1 million dollar SIR is paid by the bank. As in any clause of an insurance contract, the terms can be negotiated so a deductible does not reduce the limits.

"Occurrence" and "claims made" are two separate types of coverage bases of policies that differ as to the period protected, when claims are recognized, and when the policies are "triggered" or respond. Under an occurrence, or "loss-sustained," form the amount and type of coverage (if any) for the loss event is based on the policy that was in force when the event took place or occurred, regardless of when a claim is submitted. Under a claims-made, or "discovery," policy, the insurance policy in force when the loss event was discovered and reported to the insurance company would apply, regardless of when the event causing the claim occurred. Both types of policies have provisions regarding prompt claims-reporting to insurers. However, claims-made policies are usually stricter and their coverage may be compromised by failing to report claims in a timely manner.

Self-Insurance or Alternative Risk Transfer

There are numerous nontraditional insurance programs that larger, more complex banking organizations employ. These programs include, but are not limited to, captive insurance companies, individual or group self-insurance, risk-retention groups, and purchasing groups. These alternative risk-transfer (ART) programs are complex, and they should include common bank policies and procedures. For example, the bank should have access to individuals with insurance expertise. Outside consultants, qualified insurance brokers, and bank directors or management with insurance expertise are an integral part of a successful ART program. The ART program should also incorporate stop-loss provisions and reinsurance coverage to cap the organization's exposure to severe claims or unexpected loss experience.

COMMON POLICIES AND COVERAGES

The following is not intended to be a comprehensive list of policies and coverages available, but rather a listing and description of those that

1. An organization can maintain an unfunded reserve for loss-retention purposes.

banks most frequently purchase. The list is divided into three general types of insurance: liability, property, and life insurance. A fourth category is included for aircraft and aviation insurance, which consists of various types of property and liability coverage. While this last coverage category may be unnecessary for most banking organizations, for those institutions that do have exposure to risks associated with aircraft ownership, the risks may be exceptionally large.

Fidelity Insurance Bond

Liability insurance is sometimes called "third-party insurance" because three parties are involved in a liability loss: the insured, the insurance company, and the party (the claimant) who is injured or whose property is damaged by the insured. The insurance company pays the claimant on behalf of the insured if the insured is legally liable for the injury or damage. An insured's legal liability for injury is often the result of a negligent act, but there are other sources of liability. Several examples of liability insurance are discussed below.

Fidelity bond coverage provides reimbursement for loss from employee dishonesty; robbery; burglary; theft; forgery; mysterious disappearance; and, in specified instances, damage to offices or fixtures of the insured. Coverage applies to all banking locations except automated teller machines, for which coverage must be specifically added. All banks should obtain fidelity bond coverage that is appropriate for their business needs.

The most widely used form of fidelity bond is the Financial Institution Bond (FIB), Standard Form No. 24 (formerly named the bankers' blanket bond). Standard Form No. 24 is a claims-made, or discovery, form. The "basic" FIB has four insuring agreements or parts. Employee Dishonesty/Fidelity (Clause A) covers dishonest or fraudulent acts committed by employees. On-Premises (Clause B) covers losses from burglary, misplacement, or an unexplained disappearance that occurs on premises. In-Transit (Clause C) covers losses from burglary, misplacement, or an unexplained disappearance that occurs while the property is in transit. Counterfeit Currency (Clause F) covers losses from accepting counterfeit currency.

In addition to the basic four FIB insuring agreements, Forgery or Alteration (Clause D) and Securities (Clause E) may also appear on the standard form. (These coverages may not be a component of the most basic insurance program for a small bank.) Significant enhancements and additional coverages are often endorsed onto the FIB. Any misrepresentation, omission, concealment, or incorrect statement of material fact in the insurance application is grounds for recission of the fidelity bond by the underwriting insurance company.

When the bank under examination is a subsidiary of a bank holding company, and the holding company has purchased one fidelity bond to cover all affiliated banks, the examiner should determine that the policy is sufficient to cover the exposures of the subsidiary bank being examined. Examiners also should determine that any policy premiums the subsidiary bank pays to the parent holding company are not disproportionate to the bank's benefits from the group policy and that such premiums are consistent with the fair-market requirements of section 23B of the Federal Reserve Act. Split-limit coverage may reduce protection if a loss involves the collusion of subsidiary bank employees or other affiliates of a bank holding company.

Clause A: Fidelity (Employee Dishonesty)

Clause A covers losses resulting directly from dishonest or fraudulent acts an officer or employee commits, either acting alone or in collusion with others. The employee must have had a manifest intent to cause a loss to the financial institution, and the employee or another person or entity must obtain financial benefit from the dishonest or fraudulent act. Officers, attorneys retained by the bank, persons provided by an employment contractor, and nonemployee data processors who are performing services for the insured are typically all considered "employees." If any of the loss results from loans, that part of the loss is covered only if the employee was in collusion with other parties to the transaction and the employee received a minimum financial-benefit amount, as specified in the policy. ("Financial benefit" does not include any employee benefits earned in the normal course of employment, including salaries, commissions, fees, bonuses, promotions, awards, profit-sharing plans, or pensions.) Clause A should not

prevent the recovery of losses from employee dishonesty that are concealed by fictitious loans.

Clause B: On-Premises

Clause B covers losses of property (as defined in the bond) that occur on premises as a result of robbery, burglary, larceny, misplacement, theft, or a mysterious and unexplained disappearance. Under specified conditions, damage to offices and equipment may be covered under this clause, However, premises coverage should not be confused with standard fire or other types of property insurance.

Clause C: In-Transit

Clause C covers loss of property that is in transit. The property typically must be in the custody of (1) a natural person acting as a messenger for the insured, (2) a transportation company transporting the property in an armored motor vehicle, or (3) a transportation company transporting the property by means other than an armored motor vehicle. When an armored vehicle is not used by a transportation company, "property" is generally limited to records, certified securities, and negotiable instruments that are not payable to the bearer, are not endorsed, and have no restrictive endorsements. Some insuring agreements insure certain financial institution employees that carry cash.

Clause D: Forgery or Alteration

Clause D covers forgery, which is the signing of the name of another person or organization with the intent to deceive. Clause D also covers losses resulting from the alteration of any negotiable instrument. Evidences of debt, which the bank receives either over-the-counter or through clearings, are not usually covered. Fraudulent items received through an electronic funds transfer system are generally excluded.

Clause E: Securities

Clause E covers losses that result from a bank's extending credit or assuming liability on the faith of original securities, documents, or written instruments that are forged, altered, lost, or stolen. These include but are not limited to a certificated security, a title, a deed or mortgage, a certificate of origin or title, an evidence of debt, a security agreement, an instruction to a Federal Reserve Bank, and a statement of uncertificated security of a Federal Reserve Bank. Coverage is included for certain counterfeit securities and instruments. The bank must have acted in good faith and had actual physical possession of the original instrument.

Clause F: Counterfeit Currency

Clause F provides coverage for losses resulting from the receipt of counterfeit money. The coverage is counterfeit money of the United States, Canada, or any other country where the insured maintains a branch office.

Common FIB Extensions, Riders, or Endorsements

Fidelity bond protection can be extended by purchasing additional coverage through extensions, riders, and endorsements. If a bank has significant risk exposures in certain areas, these additional protections should be considered. The most common of these protections are listed below.

Extortion/Threats to Persons or Property

The extortion/threats to persons or property rider insures against loss of property that is surrendered away from a banking office as the result of a threat to do bodily harm to a director, trustee, employee, or relative, or of threats to damage banking premises or property. While a bank may add this coverage with a rider to its FIB, many banks purchase a separate, more comprehensive policy or endorse this coverage onto the directors' and officers' policy.

Trading Losses

The trading-loss rider amends the FIB exclusion by providing coverage for trading losses resulting directly from employee dishonesty.

Automated Teller Machines

The automated teller machine (ATM) rider covers losses of money from, or damage to, an unattended ATM that results from robbery, burglary, or theft.

Electronic or Computer Systems

The electronic or computer-systems rider covers direct losses caused by fraudulent funds transfers originated through the bank's computer systems. The fraud may be caused by a dishonest employee, customer, or third party.

Unauthorized Signatures

The unauthorized-signature rider covers losses resulting from a bank's acceptance, cashing, or payment of any negotiable instrument or withdrawal order that bears an unauthorized signature. An "unauthorized signature" is not forged, but is the signature of an individual who is not an authorized signatory on the account.

Fraudulent Mortgages

The fraudulent-mortgages rider insures against loan losses that result from a bank's accepting or acting on mortgages or deeds of trust that have defective signatures. "Defective signatures" are those obtained through fraud or trickery or under false pretenses.

Counterfeit Checks

The counterfeit-check rider insures against loss from counterfeit checks and other negotiable instruments. The coverage applies whether or not the counterfeit instruments are forged.

Service Contractors

The service-contractor rider covers loss resulting from fraudulent or dishonest acts committed by a servicing contractor. A "servicing contractor" services real estate and home-improvement mortgages, as well as tax and insurance escrow accounts; manages real property; or provides other related services. The coverage extends to losses resulting from the contractor's failure to forward collected funds to the bank when the servicing contractor has committed to do so.

Money-Order Issuer's

With a money-order-issuer's rider, coverage is expanded to authorized third parties that issue registered checks or personal money orders on behalf of the insured.

Liability Insurance

Electronic and Computer Crimes

To broaden the electronic and computer-systems rider that is normally attached to the FIB, an additional electronic and computer-crime rider may be purchased. This rider is a "companion policy" that covers losses the bank may incur from having (1) transferred, paid, or delivered any funds or property; (2) established any credit; or (3) debited any account or given value as a direct result of fraudulent input of electronic data or computer instructions into the insured's computer. These losses may result from someone's unauthorized access to a terminal or the bank's communications lines, or from the fraudulent preparation of tapes or computer programs. Under this rider, coverage may include electronic funds transfer systems, the bank's proprietary systems, and voice instructions given over the telephone. Losses caused by software programmers and consultants, ATM systems, computer viruses, software piracy, computer extortion, and facsimiles may also be covered.

Excess Bank Employee Dishonesty Bond

The excess bank employee dishonesty bond adds limits over and above the FIB. Often an FIB cannot be purchased with limits that are large enough to satisfy the risk-transfer needs of larger banks. When this occurs, the bank may purchase an excess bond that would respond if a claim is larger than the per-occurrence limits on the FIB or if the aggregate limit of the FIB has been exhausted. The most common form of this coverage is the excess bank employee dishonesty blanket bond, Standard Form No. 28.

Combination Safe Depository

Combination safe depository insurance consists of two coverage sections that can be purchased together or separately. Coverage (A) applies to losses when the bank is legally obligated to pay for loss of a customer's property held in safe deposit boxes (including loss from damage or destruction). Coverage (B) generally covers loss, damage, or destruction of property in customers' safe deposit boxes, whether or not the bank is legally liable, when the loss results from an activity other than employee dishonesty, such as robbery or burglary.

Directors' and Officers' Liability

Directors' and officers' (D&O) liability insurance usually has three coverage parts: Side A, Side B, and Entity Securities Coverage (C). Side A covers the directors and officers individually for alleged wrongful acts. Side B reimburses the bank for money it has paid to or on behalf of its directors and officers to indemnify them for damages they may be liable for as a result of alleged wrongful acts. Entity Securities Coverage protects the corporation against securities claims. Subject to many exclusions and definitions, a "wrongful act" means any actual or alleged act, error, omission, misstatement, misleading statement, neglect, or breach of duty. D&O policies are primarily written on a claims-made basis. Larger banks will purchase excess D&O coverage. Like the FIB, there are numerous coverages or enhancements that can be endorsed onto a D&O policy.

Entity errors and omissions. The entity errors and omissions (E&O) insurance rider extends coverage to the financial institution as an entity for wrongful acts. A separate, more robust E&O policy may also be purchased. The separate policy is commonly referred to as bankers' professional liability.

Fiduciary liability and ERISA errors and omissions. Fiduciary liability (or fiduciary errors and omissions) extends insurance coverage for management of the bank's own employee pension or profit-sharing plans. A separate, more robust fiduciary policy may be purchased to expand further the coverage of the bank's management of its own plans. Without this additional special endorsement, neither the fiduciary errors and omissions nor the bank's directors' and officers' liability insurance will cover liability arising under the Employee Retirement Income Security Act of 1974 (ERISA). For protection against exposure arising from a breach of fiduciary duty under ERISA, a special ERISA errors and omissions endorsement is required (also called fiduciary or employee benefit plan liability). In addition to bank trust departments, banks whose only fiduciary responsibilities relate to their employee benefit plan should consider this coverage. A related specialized coverage called IRA/Keogh errors and omissions is also available.

For properties held or managed by a bank's trust department, a master or comprehensive policy is often obtained instead of individual policies. A master policy protects the trust-account properties from fire or other loss and insures the accounts and the bank against third-party liability in connection with the properties. The master policy does not usually cover claims by trust customers against the bank for negligence, errors, or violations resulting in loss to fiduciary accounts. However, separate fiduciary (or trust department) errors and omissions policies incorporate these areas.

Trust Errors and Omissions

Trust errors and omissions insurance provides coverage for wrongful acts while the bank is acting as trustee, guardian, conservator, or administrator. This is a claims-made policy that can be endorsed onto the D&O policy.

Employment-Practices Liability

Employment-practices liability (EPL) insurance provides coverage for an entity against employee claims of wrongful termination, discrimination, sexual harassment or "wrongful employment acts." This is usually a claims-made policy that can be endorsed onto the D&O policy.

Bankers' Professional Liability

Bankers' professional liability (BPL-E&O) provides coverage for claims resulting from any actual or alleged wrongful acts, errors, or omissions bank employees commit in the performance of professional duties. Coverage can be

broadened to include securities E&O, insurance agent E&O, brokerage service E&O, and notary E&O.

Mortgage Impairment

Mortgage-impairment insurance coverage protects the bank's interest, as mortgagee, from loss when contractually required insurance on real property held as collateral has inadvertently not been obtained. Upon discovery of the lack of required coverage, the bank has a limited time to either induce the borrower to obtain the required insurance or to place the insurance on its own.

Mortgage Errors and Omissions

Mortgage errors and omissions insurance, a broader version of mortgage-impairment coverage, provides coverage for direct damage and E&O losses to either the bank or the borrower. Mortgage E&O coverage also applies to the bank's mishandling of real estate taxes, life and disability insurance, and escrowed insurance premiums. Claims must result in a loss to the mortgaged property.

Commercial General Liability

Commercial general liability (CGL) insurance protects against claims of bodily injury or property damage for which the business may be liable and which may arise from the bank's premises, operations, and products. In addition to bodily injury and property damage, CGL can include liability coverage for various other offenses that might give rise to claims, such as libel, slander, false arrest, and advertising injury. A CGL policy can be underwritten on either an occurrence or a claims-made basis.

Workers' Compensation and Employers' Liability

Workers' compensation insurance covers injuries or deaths of employees caused by accidents in the course of employment. Workers' compensation insurance consists of two basic coverage parts: statutory benefits and employers' liability (EL). The two are mutually exclusive remedies to an employee injured on the job. EL protects a company from a lawsuit filed by an employee, while statutory benefits coverage provides medical care and long-term disability, death, or other benefits. State laws govern these provisions, so the provisions differ from state to state. The statutory coverage of workers' compensation is a no-fault system intended to benefit both the injured employee and the employer.

Automobile Liability and Physical Damage

Automobile liability insurance provides third-party liability protection for bodily injury or property damage resulting from accidents that involve the bank's vehicles. First-party coverage for damage to the vehicles is also provided. This coverage should be extended to include—

- nonowned and hired coverage, if employees use personal autos or rent autos while on bank business;
- coverage for autos that have been repossessed; and
- garage-keeper's liability, if the bank rents its parking facilities to customers or the public.

Umbrella and Excess Liability

Umbrella and excess liability insurance offers additional liability limits in excess of the coverage limits of any policy over which it "attaches" or becomes effective. Basic umbrella coverage attaches to CGL and automobile insurance and to the employers' liability section of workers' compensation policies. An excess liability policy attaches over an umbrella policy. More complex insurance programs may include both umbrella and excess liability policies that attach over the D&O, E&O, EPL, or other insurance.

Property Insurance

Several types of insurance coverage are available to help banks recover from property damage. Some of the more common types of property coverages are briefly described below.

Broad Form Property Insurance

Property insurance insures against the loss of or damage to real and personal property. The loss or damage may be caused by perils such as fire, theft, windstorm, hail, explosion, riot, aircraft, motor vehicles, vandalism, malicious mischief, riot and civil commotion, and smoke.

Fire

Fire insurance covers all losses directly attributed to fire, including damage from smoke or water and chemicals used to extinguish the fire. Additional fire damage for the building contents may be included, but often is written in combination with the policy on the building and permanent fixtures. Most fire insurance policies contain "co-insurance" clauses, meaning that insurance coverage must be maintained at a fixed proportion of the replacement value of the building. If a bank fails to maintain the required relationship of protection, all losses will be reimbursed at the ratio of the amount of the insurance carried to the amount required, applied to the value of the building at the time of the loss. When determining insurable value for fire insurance purposes, the basis typically is the cost of replacing the property with a similar kind or quality at the time of loss. Different types of values, however, may be included in policies, and care should be taken to ensure that the bank is calculating the correct value for its needs.

Business Personal Property

Traditionally known as "contents" insurance, business personal property insurance affords insurance protection coverage for the furniture, fixtures, equipment, machinery, merchandise, materials, and all other personal property owned by the bank and used in its business.

Blanket Coverage

Blanket insurance covers, in a single contract, either multiple types of property at a single location or one or more types of property at multiple locations.

Builder's Risk

Builder's-risk insurance is commercial property coverage specifically for buildings that are in the course of construction.

Business Interruption

Business-interruption insurance indemnifies the insured against losses arising from its inability to continue normal operations and functions of the business. Coverage is triggered by the total or partial suspension of business operations due to the loss of, loss of use of, or damage to all or part of the bank's buildings, plant machinery, equipment, or other personal property, when the loss is the result of a covered cause.

Contingent business-interruption insurance is also available to cover the bank's loss of earnings caused by a loss to another business that is one of its major suppliers or customers. This insurance is also known as "business income from dependent properties."

Crimes

Crime insurance covers money, securities, merchandise, and other property from various criminal causes of loss, such as burglary, robbery, theft, and employee dishonesty.

Data Processing

Data processing insurance coverage provides loss protection if data processing systems break down. This insurance also covers the additional expense incurred in making the system operational again.

Difference in Conditions

A difference-in-conditions (DIC) insurance contract is a separate coverage that expands or supplements property insurance that was written on a named-perils basis. A DIC policy will cover the property on an all-risk basis, subject to certain exclusions.

Ocean and Inland Marine

Ocean marine insurance covers ships and their cargo against such causes as fire, lightning, and "perils of the seas." These include high winds, rough waters, running aground, and collision with other ships or objects.

Inland marine insurance was originally developed to provide coverage for losses to cargo transported over land. It now covers limited types of property in addition to goods in transit.

Valuable Papers and Destruction of Records

Valuable-papers and destruction-of-records insurance coverage is for the physical loss or damage to valuable papers and records of the insured. The coverage includes practically all types of printed documents or records except money.

Accounts Receivable

Accounts-receivable insurance covers losses that occur when an insured is unable to collect outstanding accounts because of damage to or destruction of the accounts-receivable records that was caused from a peril covered in the policy.

Cash Letters

Cash-letter insurance covers the costs for reproducing cash-letter items and items that remain uncollectible after a specified period of time. Generally, these policies do not cover losses due to dishonest acts of employees.

First-Class, Certified, and Registered Mail

The insurance coverage for first-class, certified, and registered mail provides protection on the shipment of property sent through the mail, as well as during transit by messenger or carrier to and from the post office. The insurance is principally used to cover registered mail in excess of the maximum $25,000 insurance provided by the U.S. Postal Service.

Commercial Multiple Peril

Commercial multiple peril insurance encompasses a range of insurance coverages, including property and liability. Small institutions may purchase this package policy when stand-alone polices are excessive or inefficient.

Life Insurance

Common types of life insurance policies purchased by banks are described below.

Key Person

When the death of a bank officer, or key person, would be of such consequence to the bank as to give it an insurable interest, key-person life insurance would insure the bank on the life of this individual.

Split-Dollar

In split-dollar life insurance, the purchaser of the policy pays at least part of the insurance premiums and is entitled to only a portion of the cash surrender value, death benefit, or both. See SR-93-37 ("Split-Dollar Life Insurance," June 18, 1993) and its attachments for further discussion of the Federal Reserve's position on these arrangements between bank holding companies and their subsidiary banks.

Bank-Owned

Bank-owned life insurance consists of tax-advantaged insurance policies that are purchased to cover the lives of bank officers and other highly compensated employees. The policies may be used as a funding mechanism for employee pension and benefit plans. The bank is the owner and beneficiary of the policy, and the cash value of the policy is considered an asset of the bank.

Aircraft or Aviation Insurance

Although aviation-liability exposures are frequently overlooked in the myriad of other finan-

cial institution exposures, they have tremendous potential for large catastrophic losses and must be addressed by senior risk-management executives at all financial institutions. Often hidden or obscure, aviation liability ranges from the more typical owned and nonowned liability and physical-damage exposures to the more exotic exposures from hangar-keepers, aviation products, and airport or heliport premises. In view of the specialized nature of aviation exposures, it is important that the bank deal with knowledgeable and experienced agents or brokers and underwriters in developing its aviation insurance program. While exposure categories overlap significantly, the following summary highlights the key areas of concern to most financial institutions.

Aviation Liability

Aviation liability insurance can be written to include aviation-products liability, all owned or nonowned exposures, and passenger liability. A bank's umbrella liability insurance program should also apply over the aviation policy's limit.

Nonowned Exposures

While many banks do not feel the need for aviation insurance because they do not own an aircraft, they may overlook liability exposures from nonowned aircraft and may, in fact, need this coverage. For example, an employee may use a personal aircraft on bank business, or lease or rent an aircraft to ferry customers or employees to a distant meeting. Financing or leasing an aircraft could create a nonowned exposure, even though the aircraft is not under bank control.

Most aviation-underwriting markets have programs available to meet the above exposures. However, additional exposures may require special coverage. Banks should consider the following situations:

- If the bank repairs and maintains the aircraft, it may incur a products-liability exposure after control is relinquished to others, such as when the aircraft is sold.
- If the bank finances aircraft, maintaining only a security interest, it becomes an owner when it repossesses the aircraft. In this case, there could be a definite need for both liability and physical-damage coverage. The coverage may be written at the time of repossession or negotiated in advance of the need for it. The bank should not attempt to continue coverage for its exposure under the borrower's policy.

All-Risk Physical Damage

To protect the bank's security interest in an aircraft hull, borrowers should be required to maintain full-value, all-risk physical-damage insurance (both ground-risk and in-flight coverage) in favor of the bank. However, a number of warranties in aircraft insurance policies could void the contract, so bankers are further advised to require that a borrower's hull insurance policy contain a breach-of-warranty endorsement to protect the bank if the borrower or owner violates provisions of the policy. The underwriter should agree to give the bank at least 30 days' advance notice of any change in the policy. Depending on the use of the aircraft, special consideration should be given to the territorial limits of coverage, as well as to confiscation protection. Since breach-of-warranty endorsements, like aircraft insurance policies, are far from standard, it is important that the bank understand and agree with the underwriter's language. It is particularly appropriate to review the consequences of potential recovery to the lien holder if the aircraft is damaged while a delinquency exists on the note.

Bank as Lessor

If the bank's security interest is that of the lessor, aviation liability insurance should be carried by the bank as lessor and also by the customer as lessee. In certain cases, it may be appropriate to require the lessee, through his or her underwriter, to provide the equivalent of the breach-of-warranty endorsement to the liability program and physical-damage coverage. The bank may also consider obtaining contingent lessor's liability.

Airport Premises and Hangar-Keepers

Airport-premises and hangar-keeper's insurance apply if the bank repossesses real estate on which an airport facility exists and continues to

operate, or if the bank permits use of the facility pending further sale. In either case, the bank may assume liability exposures associated with the control tower, as well as airport-premises liability. Both the bank's comprehensive general liability and aviation liability programs should be reviewed for proper coverage.

If the bank owns or operates a hangar for its aircraft and attempts to share the burden of costs with others by renting aircraft space, it can pick up exposure to hangar-keeper's liability, unless the contract is properly worded. Appropriate consideration should be given to hold-harmless indemnification clauses, any regular or special insurance requirements, and waivers of subrogation.

Accidental Death and Dismemberment and Travel

Accidental death and dismemberment and travel insurance is another aspect of aviation insurance that banking institutions should consider. Many insurance programs for accidental death and dismemberment and corporate business travel accidents exclude coverage in corporate-owned, -leased, or -hired aircraft. Banks need to review the language of these policies carefully to be certain that they provide necessary and adequate coverages for the use of such aircraft.

RECORDKEEPING

The diversity of available insurance policies and their coverages emphasize the need for banks to maintain a concise, easily referenced schedule of their insurance coverage, referred to as the "schedule of insurance." These records should include the following information:

- insurance coverages provided, with major exclusions detailed
- the underwriter
- deductible amounts
- upper limits on policies
- terms of the policies
- dates that premiums are due
- premium amounts
- claim-reporting procedures

In preparation for policy renewal, the bank's risk manager and insurance broker organize much of the bank's relevant insurance data into a "submission." The submission may include—

- historical, current, and forecasted exposure information, such as sales, number and type of employees, property characteristics and values, and number and type of autos;
- loss and claim history by line of insurance, including detailed information on large claims, loss development, and litigation;
- information on company risk-management policies and financials; and
- specifications on desired coverages, terms and conditions, limits, deductibles, and payment plans.

The submission is delivered to the insurance company underwriter and forms the basis for determining premiums, rates, limits, and the program structure. The information may give the examiner a sense of why premiums and coverages change from year to year and whether purchased limits are sufficient.

Banks should retain the original policies and supporting documents for appropriate time periods. Records of losses should also be maintained, regardless of whether the bank was reimbursed. This information indicates areas where internal controls may need to be improved and is useful in measuring the level of risk exposure in a particular area.

1. To determine whether insurance is effectively integrated into the operational-risk-management program, and whether the insurance is appropriate, in light of the institution's internal-control environment.
2. To determine if insurance coverage adequately protects against significant or catastrophic loss.
3. To determine if recordkeeping practices are sufficient to enable effective risk and insurance management.
4. To ascertain if, and ensure that, the risk manager has initiated corrective action when policies, practices, procedures, or internal controls are deficient or when violations of banking laws and regulations have been noted.

1. If selected for implementation, complete or update the ''Bank Risk and Insurance Management'' section of the internal control questionnaire.
2. Test for compliance with policies, practices, procedures, and internal controls in conjunction with performing the remaining examination procedures. From the examiner who is assigned to ''internal control,'' obtain a listing of any deficiencies noted in the latest review conducted by internal or external auditors and risk managers. Determine if appropriate corrections have been made.
3. Determine if the bank has designated a qualified risk manager, with expertise in insurance programs, to be responsible for loss control. If not, determine which officer handles the risk- and insurance-management function and whether external consultants are employed in designing the insurance program.
4. Obtain the bank's schedule of insurance policies in force and the renewal submissions. If the bank does not maintain a schedule, request that the bank complete a schedule of existing insurance coverage.
   a. Determine whether there have been any material changes in insurance coverage, limits, or deductibles since the last examination and the reasons for such changes. Do the changes reflect—
      - revised business strategies, the bank structure, operating processes, or technology systems that affect insurable risks, and
      - shifts to self-insurance or co-insurance or a change in insurance carriers?
   b. If there have been material changes, determine how they are being managed.
5. Using the bank-prepared summary of insurance coverage, determine that coverage conforms to the guidelines for maximum loss exposure, as established by the board of directors.
   a. Determine whether the use of insurance is in accordance with board-approved risk-management policies and guidelines.
   b. If the bank self-insures, determine what methods are used for this purpose; how the value of self-insurance is quantified; and how ''premiums'' are accounted for, funded, allocated, and tracked.
6. Determine whether insurance coverage provides adequate protection for the bank. The quality of internal controls and the audit function must be considered when making this assessment.
   a. Determine whether the bank manages its insurance coverage as an element of the operational-risk-management program.
   b. Determine whether the insurance program is managed on a corporate-wide basis or within each business unit.
   c. Identify any products, processes, or systems that the bank is not able to obtain insurance coverage for and determine how the associated risk is being managed.
   d. Determine whether the bank maintains a database of operational-loss events, the comprehensiveness of the database, and the claims history of operational losses.
   e. Review the due-diligence process used to assess the qualifications of providers of insurance coverage, including primary reinsurers.
7. If the bank's fidelity insurance has lapsed, determine that the appropriate Federal Reserve Bank has been notified.
8. Determine that the bank has adequate procedures to ensure that—
   a. reports of losses are filed with the bonding company pursuant to policy provisions,
   b. premiums are paid before policy expiration dates,
   c. policies are renewed without a lapse of coverage at expiration dates, and
   d. material changes in exposures are reported to the bank's insurance agent or broker and result in appropriate insurance-policy endorsements.

If the procedures are deficient, verify that reports have been filed as required and premiums have been paid.

9. Review any significant financial institution bond claims that were filed since the last examination to determine—

a. any adverse effect on the bank's condition,
b. whether the incident (or incidents) reflects any deficiencies with respect to internal controls and procedures, and
c. whether management has taken appropriate steps to correct any deficiencies and made appropriate reports to the board of directors.

10. Prepare, in appropriate report form, and discuss with appropriate officers—
a. recommended corrective action when policies, practices, procedures, or internal controls are deficient;
b. recommended improvements in the risk-management program that relate to insurance;
c. important areas in which insurance coverage is either nonexistent or inadequate in view of current circumstances; and
d. any other deficiencies noted.

11. Update the workpapers with any information that will facilitate future examinations.

Review the bank's internal controls, policies, practices, and procedures for its own insurance coverage. The bank's risk-management system should be documented completely and concisely and should include, where appropriate, the risk-assessment matrix, a narrative description, flowcharts, the schedule of insurance coverage, policy forms, renewal submissions, and other pertinent information.

BANK RISK AND INSURANCE MANAGEMENT

1. Does the bank have established insurance guidelines that provide for—
   a. a reasonably frequent, and at least annual, determination of risks the bank assumes or transfers, including high-dollar and low-probability events?
   b. limits as to the amount of risk that may be retained or self-insured?
   c. periodic appraisals of major fixed assets to be insured?
   d. a credit or financial analysis of the insurance companies who have issued policies to the bank?
2. Does the bank have a risk manager who is responsible for assessing and developing controls to deal with the consolidated risks of the institution?
3. Is the bank's insurance program managed as an element of its overall operational-risk-management program; that is, are insurance coverages reviewed and coordinated by the person handling the operational-risk-management function?
4. Does the bank use the services of a professionally knowledgeable insurance agent, broker, direct writer, or consultant to assist in selecting and providing advice on alternative means of providing insurance coverage?
5. Does the bank's security officer coordinate his or her activities with the person responsible for handling the operational-risk-management function?
6. Does the bank maintain a concise, easily referenced schedule of existing insurance coverage?
7. Does the bank maintain records, by type of risk, to facilitate an analysis of the bank's experience in costs, claims, losses, and settlements under the various insurance policies in force?
8. Is a complete schedule of insurance coverage presented to the board of directors at least annually for review and approval? Does the schedule include the respective insurance premiums (net costs), claims, and loss experience, and is this information reviewed as part of this process?

CONCLUSION

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

State member banks may purchase bank-owned life insurance (BOLI) as principal if such purchases are permitted for national banks and permitted under state law. The legal authority and guidance for acquiring permissible BOLI and for engaging in insurance activities is discussed within the following interagency statement. When such insurance purchases or insurance activities are not permissible for national banks, a determination of permissibility depends on a decision of the FDIC (1) that the investment or activity would not pose any significant risk to the insurance fund and (2) that the bank continues to comply with the required capital standards.

The bank supervisory agencies have concerns that some banks have committed a significant amount of capital to BOLI without having an adequate understanding or a proper assessment of the full array of risks it poses—especially risks that are difficult to measure, such as liquidity, transaction/operational, reputation, and compliance/legal risks. Banks are therefore expected to implement appropriate risk-management processes, including meaningful risk limits, before implementing or adding to a BOLI program. The following interagency guidance was developed for banks and savings associations (institutions) and examination staff to help ensure that risk-management practices for BOLI are consistent with safe and sound business practices. The interagency statement was issued on December 7, 2004.

INTERAGENCY STATEMENT ON THE PURCHASE AND RISK MANAGEMENT OF LIFE INSURANCE

This interagency statement[1] provides general guidance for banks and savings associations (institutions) regarding supervisory expectations for the purchase of and risk management for BOLI. Guidance is also provided for split-dollar arrangements and the use of life insurance as security for loans. The agencies are providing this guidance to help ensure that institutions' risk-management processes for BOLI are consistent with safe and sound banking practices. Among the safe and sound banking practices discussed in this statement are (1) the need for senior management and board oversight of BOLI, including both a thorough pre-purchase analysis of risks and rewards and post-purchase risk assessment and (2) the permissibility of BOLI purchases and holdings, as well as their risks and associated safety-and-soundness considerations. The statement's appendix [titled appendix A for this section of the manual] contains a discussion of insurance types and the purposes for which institutions commonly purchase life insurance, as well as a glossary of BOLI-related terminology [titled appendix B for this section].

The statement's guidance for the pre-purchase analysis of life insurance applies to all BOLI contracts entered into after December 7, 2004. The guidance concerning the ongoing risk management of BOLI subsequent to its purchase applies to all holdings of life insurance regardless of when purchased. Institutions that purchase life insurance after December 7, 2004, that are not in compliance with this guidance may be subject to supervisory action. Institutions that entered into BOLI contracts before this date will be evaluated according to each agency's pre-purchase guidance in effect at that time.

Compliance with the supervisory guidance in this statement regarding permissible uses for insurance (e.g., recovery of the costs of providing benefits) does not determine whether the policy satisfies state insurable interest requirements.

Legal Authority

National banks may purchase and hold certain types of life insurance under 12 USC 24 (Seventh), which provides that national banks may exercise "all such incidental powers as shall be necessary to carry on the business of banking." Federal savings associations also may purchase and hold certain types of life insurance incidental to the express powers granted under the Home Owners' Loan Act. The OCC and OTS have delineated the scope of these authorities through various interpretations addressing the

1. Adopted by the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS) (the agencies).

permissible use of life insurance by national banks and federal savings associations.

Under these authorities, national banks and federal savings associations may purchase life insurance in connection with employee compensation and benefit plans, key-person insurance, insurance to recover the cost of providing pre- and post-retirement employee benefits, insurance on borrowers, and insurance taken as security for loans. The OCC and OTS may approve other uses on a case-by-case basis.

National banks and federal savings associations may *not* purchase life insurance—

- for speculation;
- to provide funds to acquire shares of stock from the estate of a major shareholder upon the shareholder's death, for the further purpose of controlling the distribution of ownership in the institution;
- as a means of providing estate-planning benefits for insiders, unless the benefit is a part of a reasonable compensation package; or
- to generate funds for normal operating expenses other than employee compensation and benefits.

National banks and federal savings associations may not hold life insurance in excess of their risk of loss or cost to be recovered. For example, once an individual no longer qualifies as a key person because of retirement, resignation, discharge, change of responsibilities, or for any other reason, the risk of loss has been eliminated. Therefore, national banks and federal savings associations may be required to surrender or otherwise dispose of key-person life insurance held on an individual who is no longer a key person. Typically, term or declining term insurance is the most appropriate form of life insurance for key-person protection.

National banks and federal savings associations may hold equity-linked variable life insurance policies (that is, insurance policies with a return tied to the performance of a portfolio of equity securities held in a separate account[2] of the insurance company) only for the purpose of economically hedging their equity-linked obligations under employee benefit plans. As discussed more fully in the section on "Price Risk," for equity-linked variable life insurance holdings to be permissible, the national bank or federal savings association must demonstrate that—

- it has a specific, equity-linked obligation; and
- both at the inception of the hedge and on an ongoing basis, changes in the value of the equity-linked variable life insurance policy are highly correlated with changes in the value of the equity-linked obligation.

If a national bank or federal savings association does not meet these requirements, the equity-linked variable life insurance holdings are not permissible. The use of equity-linked variable life insurance holdings as a long-term hedge against general benefit costs is not permissible because the life insurance is not hedging a specific equity-linked liability and does not meet the "highly correlated" requirement.

As a general matter, the ability of state-chartered banks to purchase insurance (including equity-linked variable life insurance) is governed by state law. In some instances, state laws permit state-chartered banks to engage in activities (including making investments) thatgo beyond the authority of a national bank. The Federal Deposit Insurance Act (section 24) generally requires insured state-chartered banks to obtain the FDIC's consent before engaging as principal in activities (including making investments) that are not permissible for a national bank. Similarly, the Federal Deposit Insurance Act (section 28) generally requires a state-chartered savings association to obtain the FDIC's consent prior to engaging as principal in activities (including making investments) that are not permissible for a federal savings association. While insured state-chartered banks and state savings associations may seek the FDIC's consent to make purchases of life insurance that would not be within the authority of a national bank or federal savings association, such banks and savings associations should be aware that the FDIC will not grant permission to make life insurance purchases if the FDIC determines that doing so would present a significant risk to the deposit insurance fund or that engaging in such

2. A separate account is a design feature that is generally available to purchasers of whole life or universal life whereby the policyholder's cash surrender value is supported by assets segregated from the general assets of the carrier. Under such an arrangement, the policyholder neither owns the underlying separate account nor controls investment decisions (e.g., timing of investments or credit selection) in the underlying separate account that is created by the insurance carrier on its behalf. Nevertheless, the policyholder assumes all investment and price risk.

purchases is inconsistent with the purposes of federal deposit insurance.

Accounting Considerations

Institutions should follow generally accepted accounting principles (GAAP) applicable to life insurance for financial and regulatory reporting purposes. Financial Accounting Standards Board (FASB) Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance" (TB 85-4), discusses how to account for holdings of life insurance. Under TB 85-4, only the amount that could be realized under an insurance contract as of the balance-sheet date (that is, the CSV reported to the institution by the carrier, less any applicable surrender charges not reflected by the insurance carrier in the reported CSV) is reported as an asset. The guidance set forth in TB 85-4 concerning the carrying value of insurance on the balance sheet is generally appropriate for all forms of BOLI.

An institution may purchase multiple permanent insurance policies from the same insurance carrier with each policy having its own surrender charges. In some cases, the insurance carrier will issue a rider or other contractual provision stating that it will waive the surrender charges if all of the policies are surrendered at the same time. Because it is not known at any balance-sheet date whether one or more of the policies will be surrendered before the deaths of those insured, the possibility that the institution will surrender all of these policies simultaneously and avoid the surrender charges is a gain contingency. Under FASB Statement No. 5, "Accounting for Contingencies," "[c]ontingencies that might result in gains usually are not reflected in the accounts since to do so might be to recognize revenue prior to its realization." Accordingly, an institution should report each of the insurance policies on its balance sheet at the policy's CSV reported by the insurance carrier, less any applicable surrender charges not reflected in the reported CSV, without regard to the existence of the rider.

In accordance with the instructions for Consolidated Reports of Condition and Income and Thrift Financial Reports, an institution should report the carrying value of its BOLI holdings as an "other asset" and the earnings on these holdings should be reported as "other noninterest income."

The agencies have seen a number of cases in which institutions have failed to account properly for a type of deferred compensation agreement, commonly referred to as a revenue-neutral plan or an indexed retirement plan. The accounting for such plans is separate and distinct from the accounting for BOLI. However, because many institutions buy BOLI to help offset the cost of providing such deferred compensation, the agencies have issued guidance addressing the accounting requirements for both deferred compensation agreements and BOLI. See the Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance, dated February 11, 2004, for a complete description, including examples, of the appropriate accounting treatment.

Supervisory Guidance on BOLI

Before entering into a BOLI contract, institutions should have a comprehensive risk-management process for purchasing and holding BOLI. A prudent risk-management process includes—

- effective senior management and board oversight;
- comprehensive policies and procedures, including appropriate limits;
- a thorough pre-purchase analysis of BOLI products; and
- an effective ongoing system of risk assessment, management, monitoring, and internal control processes, including appropriate internal audit and compliance frameworks.

The risks associated with temporary (term) insurance are significantly less than those arising from holdings of permanent insurance. Accordingly, the risk-management process for temporary insurance may take this difference into account and need not be as extensive as the risk-management process for permanent insurance.

Senior Management and Board Oversight

The safe and sound use of BOLI depends on effective senior management and board oversight. Regardless of an institution's financial capacity and risk profile, the board must under-

stand the complex risk characteristics of the institution's insurance holdings and the role this asset is intended to play in the institution's overall business strategy. Although the board may delegate decision-making authority related to purchases of BOLI to senior management, the board remains ultimately responsible for ensuring that the purchase and holding of BOLI is consistent with safe and sound banking practices.

An institution holding life insurance in a manner inconsistent with safe and sound banking practices is subject to supervisory action. Where ineffective controls over BOLI risks exist, or the exposure poses a safety-and-soundness concern, the appropriate agency may take supervisory action against the institution, including requiring the institution to divest affected policies, irrespective of potential tax consequences.

Policies and Procedures

Consistent with prudent risk-management practices, each institution should establish internal policies and procedures governing its BOLI holdings, including guidelines that limit the aggregate CSV of policies from any one insurance company as well as the aggregate CSV of policies from all insurance companies. When establishing these internal CSV limits, an institution should consider its legal lending limit, the capital concentration threshold, and any applicable state restrictions on BOLI holdings.[3] In this regard, given the liquidity, transaction/operational, reputation, and compliance/legal risks associated with BOLI, it is generally not prudent for an institution to hold BOLI with an aggregate CSV that exceeds 25 percent of the institution's capital as measured in accordance with the relevant agency's concentration guidelines.[4] Therefore, the agencies expect an institution that plans to acquire BOLI in an amount that results in an aggregate CSV in excess of 25 percent of capital, or any lower internal limit, to gain prior approval from its board of directors or the appropriate board committee. The agencies particularly expect management to justify that any increase in BOLI resulting in an aggregate CSV above 25 percent of capital does not constitute an imprudent capital concentration. An institution holding BOLI in an amount that approaches or exceeds the 25 percent of capital concentration threshold can expect examiners to more closely scrutinize the risk-management policies and controls associated with the BOLI assets and, where deficient, to require corrective action.

When seeking the board's approval to purchase or increase BOLI, management should inform the board members of the existence of this interagency statement, remind them of the illiquid nature of the insurance asset, advise them of the potential adverse financial impact of early surrender, and identify any other significant risks associated with BOLI. Such risks might include, but are not limited to, the costs associated with changing carriers in the event of a decline in the carrier's creditworthiness and the potential for noncompliance with state insurable interest requirements and federal tax law.

Pre-purchase Analysis

The objective of the pre-purchase analysis is to help ensure that the institution understands the risks, rewards, and unique characteristics of BOLI. The nature and extent of this analysis should be commensurate with the size and complexity of the potential BOLI purchases and should also take into account existing BOLI holdings. A mark of a well-managed institution is the maintenance of adequate records concerning its pre-purchase analyses, usually including documentation of the purpose and amount of insurance needed.

An effective pre-purchase analysis involves the following management actions:

Step 1—Identify the need for insurance and determine the economic benefits and appropriate insurance type. An institution should deter-

3. In July 1999, the OTS adopted a policy that savings associations may not invest more than 25 percent of their total capital in BOLI without first notifying and obtaining authorization from their OTS Regional Office. In order to maintain strong and effective communications with institutions under its supervision, the OTS retains this policy. The other agencies may also institute approval or notification requirements.

4. Each agency's definition of a concentration differs slightly. Institutions should refer to the definition provided by their supervisory agency when measuring the CSV of BOLI as a percentage of capital: OCC Bulletin 95-7 for national banks; FRB *Commercial Bank Examination Manual,* section 2050.1, for state member banks; FDIC *Manual of Examination Policies,* section 11.1, for insured state nonmember banks; and OTS *Thrift Activities Handbook,* section 211, for savings associations.

mine the need for insurance by identifying the specific risk of loss to which it is exposed or the specific costs to be recovered. It is not appropriate to purchase life insurance to recover a loss that the institution has already incurred. An institution's purchase of insurance to indemnify it against a specific risk of loss does not relieve it from other responsibilities related to managing that risk. The type of BOLI product, e.g., general[5] or separate account, and its features should be appropriate to meet the identified needs of the institution. The appendix [appendix A] contains a description of insurance types and design features.

An institution should analyze the cost and benefits of planned BOLI purchases. The analysis should include the anticipated performance of the BOLI policy and an assessment of how the purchase will accomplish the institution's objectives. Before purchasing BOLI, an institution should analyze projected policy values (CSV and death benefits) using multiple illustrations of these projections provided by the carrier, some of which incorporate the institution's own assumptions. An institution should consider using a range of interest-crediting rates and mortality-cost assumptions. In some cases, the net yield (after mortality costs) could be negative, particularly for separate-account products. The potential for unfavorable net yields underscores the importance of carefully evaluating BOLI costs and benefits across multiple scenarios, both currently and into the future.

Step 2—Quantify the amount of insurance appropriate for the institution's objectives. An institution should estimate the size of the employee benefit obligation or the risk of loss to be covered and ensure that the amount of BOLI purchased is not excessive in relation to this estimate and the associated product risks. When using BOLI to recover the cost of providing employee benefits, the estimated present value of the expected future cash flows from BOLI, less the costs of insurance, should not exceed the estimated present value of the expected after-tax employee benefit costs. In situations where an institution purchases BOLI on a group of eligible employees, it may estimate the size of the obligation or the risk of loss for the group on an aggregate basis and compare that to the aggregate amount of insurance to be purchased. This estimate should be based on reasonable financial and actuarial assumptions. State insurable interest laws may further restrict or limit the amount of insurance that may be purchased on a group of employees. Management must be able to support, with objective evidence, the reasonableness of all of the assumptions used in determining the appropriate amount of insurance coverage needed by the institution, including the rationale for its discount rates and cost projections.

Step 3—Assess the vendor's qualifications. When making a decision about vendors, an institution should consider its own knowledge of insurance risks, the vendor's qualifications, and the amount of resources the institution is willing to spend to administer and service the BOLI. Depending on the role of the vendor, the vendor's services can be extensive and may be critical to successful implementation and operation of a BOLI plan, particularly for the more complex separate-account products.

While it is possible to purchase insurance directly from insurance carriers, the vast majority of insurance purchases are made through vendors—either brokers, consultants, or agents. A vendor may design, negotiate, and administer the BOLI policy. An institution should ensure that it understands the product it is purchasing and that it selects a product that best meets its needs. Management, not just the vendor, must demonstrate a familiarity with the technical details of the institution's insurance assets, and be able to explain the reasons for and the risks associated with the product design features they have selected.

An institution that uses a vendor should make appropriate inquiries to satisfy itself about the vendor's ability to honor its long-term commitments, particularly when the vendor is expected to be associated with the institution's insurance program over an extended period of time. The institution should evaluate the adequacy of the vendor's services and its reputation, experience, financial soundness, and commitment to the BOLI product. Vendors typically earn a large portion of their commissions upon the sale of the product, yet they often retain long-term servicing responsibilities for their clients. The vendor's commitment to investing in the operational infrastructure necessary to support BOLI is a key consideration in vendor selection.

5. A general account is a design feature that is generally available to purchasers of whole or universal life insurance whereby the general assets of the insurance company support the policyholder's CSV.

An institution should be aware that the vendor's financial benefit from the sale of insurance may provide the vendor with an incentive to emphasize the benefits of a BOLI purchase to the institution without a commensurate explanation of the associated risks. Therefore, reliance solely upon pre-packaged, vendor-supplied compliance information does *not* demonstrate prudence with respect to the purchase of insurance. An institution should not delegate its selection of product design features to its vendors. An institution that is unable to demonstrate a thorough understanding of BOLI products it has purchased and the associated risks may be subject to supervisory action.

Step 4—Review the characteristics of the available insurance products. There are a few basic types of life insurance products in the marketplace. These products, however, can be combined and modified in many different ways. The resulting final product can be quite complex. Furthermore, certain permanent insurance products have been designed specifically for banks. These products differ from other forms of corporate-owned life insurance (COLI) policies in that the policies designed for banks are generally structured without surrender or front-end sales charges in order to avoid having to report these charges as expenses when initially recording the carrying value. However, BOLI products may have lower net yields than COLI products due to the absence of these charges. An institution should review the characteristics of the various insurance products available, understand the products it is considering purchasing, and select those with the characteristics that best match the institution's objectives, needs, and risk tolerance.

Design features of permanent insurance policies determine (1) whether the policy is a general account, separate account, or hybrid product;[6] (2) whether the insurance contract is a modified endowment contract (MEC) that carries certain tax penalties if surrendered; and (3) the method used to credit earnings to the policy. Some implications of these design features are discussed in more detail in the "Risk Management of BOLI" section of this interagency statement.

When purchasing insurance on a key person or a borrower, management should consider whether the institution's need for the insurance might end before the insured person dies. An institution generally may not hold BOLI on a key person or a borrower once the key person leaves the institution or the borrower has either repaid the loan, or the loan has been charged off. Therefore, the maturity of the term or declining term insurance should be structured to match the expected tenure of the key person or the maturity of the loan, respectively. Permanent insurance generally is not an appropriate form of life insurance under these circumstances.

Step 5—Select the carrier. To achieve the tax benefits of insurance, institutions must hold BOLI policies until the death of the insured. Therefore, carrier selection is one of the most critical decisions in a BOLI purchase and one that can have long-term consequences. While a broker or consultant may assist the institution in evaluating carrier options, the institution alone retains the responsibility for carrier selection. Before purchasing life insurance, an institution should perform a credit analysis on the selected carrier(s) in a manner consistent with safe and sound banking practices for commercial lending. A more complete discussion of the credit-analysis standards is included in the "Credit Risk" section of this interagency statement.

Management should review the product design, pricing, and administrative services of proposed carriers and compare them with the institution's needs. Management should also review the carrier's commitment to the BOLI product, as well as its credit ratings, general reputation, experience in the marketplace, and past performance. Carriers not committed to general-account BOLI products may have an incentive to lower the interest-crediting rate on BOLI over time, reducing the favorable economics of the product. The interest-crediting rate refers to the gross yield on the investment in the insurance policy, that is, the rate at which the cash value increases before considering any deductions for mortality cost, load charges, or other costs that are periodically charged against the policy's cash value. Insurance companies frequently disclose both a current interest-crediting rate and a guaranteed minimum interest-crediting rate. Institutions should be aware that the guaranteed minimum interest-crediting rate may be periodically reset in accordance with the terms of the insurance contract. As a result, the potential exists for a decline in the interest-crediting rate.

6. A hybrid product combines features of both general- and separate-account products.

While institutions can exercise what is known as a 1035 exchange[7] option to change carriers, there are some practical constraints to using this option. First, the institution must have an insurable interest in each individual to be insured under the new carrier's policy. In a 1035 exchange, former employees of the institution may not be eligible for coverage under the new policy because state insurable interest laws may prohibit their eligibility. Second, the original carrier may impose an exchange fee specifically applicable to such 1035 exchanges.

Step 6—Determine the reasonableness of compensation provided to the insured employee if the insurance results in additional compensation. Insurance arrangements that are funded by the institution and that permit the insured officer, director, or employee to designate a beneficiary are a common way to provide additional compensation or other benefits to the insured. Split-dollar life insurance arrangements are often used for this purpose. Before an institution enters into a split-dollar arrangement or otherwise purchases insurance for the benefit of an officer, director, or employee, the institution should identify and quantify its compensation objective and ensure that the arrangement is consistent with that objective. The compensation provided by the split-dollar or other insurance arrangement should be combined with all other compensation provided to the insured to ensure that the insured's total compensation is not excessive. Excessive compensation is considered an unsafe and unsound banking practice. Guidelines for determining excessive compensation can be found in the Interagency Guidelines Establishing Standards for Safety and Soundness.[8]

Because shareholders and their family members who are not officers, directors, or employees of an institution do not provide goods or services to the institution, they should not receive compensation from the institution. This includes compensation in the form of split-dollar life insurance arrangements.

Prior to an institution's purchase of a life insurance policy to be used in a split-dollar life insurance arrangement, the institution and the insured should enter into a written agreement. Written agreements usually describe the rights of the institution, the insured individual, and any other parties (such as trusts or beneficiaries) to the policy's CSV and death benefits. It is important for an institution to be aware that ownership of the policy by the employee, a third party, or a trust (non-institution owner) may not adequately protect the institution's interest in the policy because the institution ordinarily will not have the sole right to borrow against the CSV or to liquidate the policy in the event that funds are needed to provide liquidity to the institution. Moreover, if a non-institution owner borrows heavily against the CSV, an institution's ability to recover its premium payments upon the death of the insured may be impaired.

At a minimum, an institution's economic interest in the policy should be equal to the premiums paid plus a reasonable rate of return, defined as a rate of return that is comparable to returns on investments of similar maturity and credit risk.

Split-dollar life insurance has complex tax and legal consequences. An institution considering entering into a split-dollar life insurance arrangement should consult qualified tax, legal, and insurance advisers.

Step 7—Analyze the associated risks and the ability to monitor and respond to those risks. An institution's pre-purchase analysis should include a thorough evaluation of all significant risks, as well as management's ability to identify, measure, monitor, and control those risks. An explanation of key risks (liquidity, transaction/operational, reputation, credit, interest rate, compliance/legal, and price) is included in the "Risk Management of BOLI" section of this interagency statement.

Step 8—Evaluate the alternatives. Regardless of the purpose of BOLI, a comprehensive pre-purchase analysis will include an analysis of available alternatives. Prior to acquiring BOLI, an institution should thoroughly analyze the risks and benefits, compared to alternative methods for recovering costs associated with the loss of key persons, providing pre- and post-retirement employee benefits, or providing additional employee compensation, as appropriate.

7. A 1035 exchange is a tax-free replacement of an insurance policy for another insurance contract covering the same person in accordance with section 1035 of the Internal Revenue Code.

8. For national banks, appendix A to 12 CFR 30; for state member banks, appendix D-1 to 12 CFR 208; for insured state nonmember banks, appendix A to 12 CFR 364; for savings associations, appendix A to 12 CFR 570.

Step 9—Document the decision. A well-managed institution maintains adequate documentation supporting its comprehensive pre-purchase analysis, including an analysis of both the types and design of products purchased and the overall level of BOLI holdings.

Risk Management of BOLI

Risk assessment and risk management are vital components of an effective BOLI program. In addition to conducting a risk assessment as part of a thorough pre-purchase analysis, monitoring BOLI risks on an ongoing basis is important, especially for an institution whose aggregate BOLI holdings represent a capital concentration. Management of an institution should review the performance of the institution's insurance assets with its board of directors at least annually. More-frequent reviews are appropriate if there are significant anticipated changes to the BOLI program such as additional purchases, a decline in the financial condition of the insurance carrier(s), anticipated policy surrenders, or changes in tax laws or interpretations that could have an impact on the performance of BOLI. This risk-management review should include, but not necessarily be limited to:

- *Comprehensive assessment of the specific risks discussed in this section.*[9]
- *Identification of which employees are, or will be, insured (e.g., vice presidents and above, employees of a certain grade level).* For example, an institution that acquires another institution that owns BOLI may acquire insurance on individuals that it would not insure under its own standards. While the acquiring institution need not correct such exceptions, it is important to know that such exceptions exist.
- *Assessment of death benefit amounts relative to employee salaries.* Such information helps management to assess the reputation and insurable interest risks associated with disproportionately large death benefits.
- *Calculation of the percentage of insured persons still employed by the institution.* Larger institutions often find that their policies insure more former employees than current employees. This information can help the institution assess reputation risk.
- *Evaluation of the material changes to BOLI risk-management policies.*
- *Assessment of the effects of policy exchanges.* Exchanges typically are costly and it is a sound practice to review the costs and benefits of such actions.
- *Analysis of mortality performance and impact on income.* Material gains from death benefits can create reputation risks.
- *Evaluation of material findings from internal and external audits and independent risk-management reviews.*
- *Identification of the reason for, and tax implications of, any policy surrenders.* In some cases, institutions have surrendered BOLI policies and incurred tax liabilities and penalties. Formal assessment of the costs and benefits of a surrender is a useful component of sound corporate governance.
- *Peer analysis of BOLI holdings.* To address reputation risk, an institution should compare its BOLI holdings relative to capital to the holdings of its peers to assess whether it is an outlier.

Liquidity Risk

Liquidity risk is the risk to earnings and capital arising from an institution's inability to meet its obligations when they come due without incurring unacceptable losses. Before purchasing permanent insurance, management should recognize the illiquid nature of the product and ensure that the institution has the long-term financial flexibility to hold the asset in accordance with its expected use. The inability to hold the life insurance until the death(s) of the insured(s) when the death benefits will be collected may compromise the success of the BOLI plan. An institution generally does not receive any cash flow from the insurance until the death benefit is paid. Depending upon the age of the insured population, it is possible that an institution that insures a small number of employees may not recognize any cash flow from the insurance for many years. The illiquid nature of insurance assets, combined with the difficulty of projecting liquidity needs far into the future, is a major reason an institution should keep its BOLI holdings below the agencies' concentration

9. All of the risks discussed in this section are applicable to permanent insurance. In contrast, because temporary insurance does not have a savings component or a CSV, it does not expose an institution to liquidity, interest-rate, or price risk. These risks need not be evaluated in the comprehensive assessment of the risks of temporary insurance.

guidelines. Examiners will consider an institution's BOLI holdings when assessing liquidity and assigning the liquidity component rating.

The purchase of BOLI may negatively affect an institution's liquidity position, both because BOLI is one of the least liquid assets on an institution's balance sheet, and because institutions normally fund BOLI purchases through the sale of liquid assets (e.g., marketable securities). To access the CSV of BOLI, the institution must either surrender or borrow against the policy. In accordance with the policy contract and federal tax laws, the surrender of a policy may subject an institution to surrender charges, tax liabilities for previously untaxed increases in the CSV, and tax penalties. Borrowing against the CSV is disadvantageous in most cases due to limitations on the ability to deduct interest on the borrowing and other possible adverse tax consequences.

A BOLI product qualifying as a modified endowment contract (MEC) for tax purposes has particular liquidity disadvantages. If an institution surrenders a MEC, it will incur a tax liability on the increase in the policy's CSV from earnings on the policy since its inception and may incur an additional tax penalty for early surrender.

In order to avoid such additional tax penalties, an institution may opt to purchase a non-MEC contract. A non-MEC contract permits the policy owner to surrender the policy without incurring the additional tax penalty that, under certain circumstances, applies to MECs. Moreover, depending on the terms of the insurance contract, an institution generally may withdraw up to the basis (that is, the original amount invested) without creating a taxable event. However, a non-MEC policy increases in complexity if it is in the form of a separate account covered by a stable value protection (SVP) contract. An SVP contract protects the policy owner from declines in the value of the assets in the separate account arising from changes in interest rates, thereby mitigating price risk and earnings volatility. An SVP contract is most often used in connection with fixed-income investments. Institutions should recognize that SVP providers often place restrictions on the amount that may be withdrawn from the separate account, thereby reducing the liquidity of the BOLI asset. An institution considering the purchase of a non-MEC for its potential liquidity advantages compared to a MEC also should be aware of contractual provisions, such as 1035 exchange fees and "crawl-out" restrictions,[10] which may limit such advantages.

Transaction/Operational Risk

As it applies to BOLI, transaction/operational risk is the risk to earnings and capital arising from problems caused by the institution's failure to fully understand or to properly implement a transaction. Transaction/operational risk arises due to the variety and complexity of life insurance products, as well as tax and accounting treatments. To help mitigate this risk, management should have a thorough understanding of how the insurance product works and the variables that dictate the product's performance. The variables most likely to affect product performance are the policy's interest-crediting rate, mortality cost, and other expense charges.

Transaction/operational risk is also a function of the type and design features of a life insurance contract. With a general-account product, there are only two parties to the contract: the policy owner and the insurance carrier. With a separate-account product, the insurance carrier has a separate contract with an investment manager. There could also be an SVP provider with whom the carrier has a separate contract.

Transaction/operational risk may also arise as a result of the variety of negotiable features associated with a separate-account product. These include the investment options; the terms, conditions, and cost of SVP; and mortality options. Deferred acquisition costs (DAC) represent the insurance carrier's up-front costs associated with issuing an insurance policy, including taxes and commissions and fees paid to agents for selling the policy. The carrier charges the policyholder for these costs and capitalizes the DAC, including the prepayment of taxes in accordance with federal tax law. As the carrier recovers the DAC in accordance with applicable tax law, it credits the amount to the separate-account policyholder. Once it has been credited to the institution, the DAC is essentially a receivable from the carrier and, therefore, represents a general-account credit exposure.

Separate-account policies have additional transaction risks that can result from accounting requirements. Several institutions have had to

10. A crawl-out restriction limits the amount of CSV eligible for a 1035 exchange or surrender over a period of time.

restate their earnings because of contractual provisions in their policies that were ambiguous with respect to the amount of the CSV available upon surrender of the policy. Because BOLI must be carried at the amount that could be realized under the insurance contract as of the balance-sheet date, if any contractual provision related to costs, charges, or reserves creates uncertainty regarding the realization of a policy's full CSV, the agencies will require an institution to record the BOLI net of those amounts. As part of an effective pre-purchase analysis, an institution should thoroughly review and understand how the accounting rules will apply to the BOLI policy it is considering purchasing.

Tax and Insurable Interest Implications

Before the purchase of BOLI and periodically thereafter, management should also explicitly consider the financial impact (e.g., tax provisions and penalties) of surrendering a policy. Recent adverse press coverage of corporate-owned life insurance (COLI) should serve as a reminder to institutions that the current tax law framework, as it applies to BOLI, is always subject to legislative changes. A tax change that makes future BOLI cash flows subject to income tax, while perhaps deemed unlikely by many institutions, would have a negative impact on the economics of the BOLI holdings. An institution should recognize that earnings from BOLI could make it subject to the alternative minimum tax.

Institutions should also recognize that their actions, subsequent to purchase, could jeopardize the tax-advantaged status of their insurance holdings. The risk that a life insurance policy could be characterized by the Internal Revenue Service (IRS) as an actively managed investment is particularly relevant to separate-account policies. Many larger institutions prefer separate-account products because of perceived lower credit risk and greater transparency (that is, explicit disclosure of costs). Assets held by the insurance company on behalf of the policy owners in the separate account are intended to be beyond the reach of the insurance company's general creditors in the event of insolvency; however, the protected status of separate-account assets is generally untested in the courts. While the separate-account structure helps to mitigate an institution's credit exposure to the insurance carrier, the institution can have no "control" over investment decisions (e.g., timing of investments or credit selection) in the underlying account. Generally, allocating separate-account holdings across various divisions of an insurance company's portfolio does not raise concerns about "control," but other actions that a policy owner takes may be construed as investment control and could jeopardize the tax-advantaged status.

To benefit from the favorable tax treatment of insurance, a BOLI policy must be a valid insurance contract under applicable state law and must qualify under applicable federal law. Institutions must have an insurable interest in the covered employee, as set forth in applicable state laws. Furthermore, the favorable tax-equivalent yields of BOLI result only when an institution generates taxable income. Institutions that have no federal income tax liability receive only the nominal interest-crediting rate as a yield. In such an environment, BOLI loses much of its yield advantage relative to other investment alternatives.

Some institutions seem to have drawn comfort from assurances from insurance carriers that the carrier would waive lack of insurable interest as a defense against paying a claim. While the carrier may indeed make a payment, such payment may not necessarily go to the institution. Such assurances may not be sufficient to satisfy the IRS requirements for a valid insurance contract, nor do they eliminate potential claims from the estate of the insured that might seek to claim insurance proceeds on the basis that the institution lacked an insurable interest.

For example, some institutions have established out-of-state trusts to hold their BOLI assets. While such trusts may have legitimate uses, such as to gain access to an insurance carrier's product, in some cases the purpose is to avoid unfavorable insurable interest laws in the institution's home state and to domicile the policy in a state with more lenient requirements. In some cases, institutions have not made employees aware that they have taken out insurance on their lives.

A recent Fifth Circuit Court of Appeals ruling demonstrates the potential danger of this approach. A Texas employer used a Georgia trust to hold life insurance policies on its employees in Texas, and the trust agreement provided that the insurable interest law of Georgia should apply. In a lawsuit brought by the estate of a deceased employee, the court ignored this pro-

vision because the insured employee was not a party to the trust agreement. It then found that the insurable interest law of Texas applied and under that state's law, the employer did not have an insurable interest in the employee. The result was that the employer was not entitled to the insurance death benefits.[11] The outcome in this case suggests that institutions that have used, or are considering using, an out-of-state trust to take advantage of more-favorable insurable interest laws in another state should assess whether they could be vulnerable to a similar legal challenge.

Institutions should have appropriate legal review to help ensure compliance with applicable tax laws and state insurable interest requirements. Institutions that insure employees for excessive amounts may be engaging in impermissible speculation or unsafe and unsound banking practices. The agencies may require institutions to surrender such policies.

Reputation Risk

Reputation risk is the risk to earnings and capital arising from negative publicity regarding an institution's business practices. While this risk arises from virtually all bank products and services, reputation risk is particularly prevalent in BOLI because of the potential perception issues associated with an institution's owning or benefiting from life insurance on employees.

A well-managed institution will take steps to reduce the reputation risk that may arise as a result of its BOLI purchases, including maintaining appropriate documentation evidencing informed consent by the employee, prior to purchasing insurance. Some institutions assert that they make employees aware via employee handbooks, manuals, or newsletters of the possibility that the institution may acquire life insurance on them. Although such disclosure may satisfy state insurance requirements, any approach that does not require formal employee consent may significantly increase an institution's reputation risk.

Some institutions have begun to purchase separate-account, non-MEC product designs in order to address the liquidity concerns with MEC policies. One consequence of this product design choice, however, is that it has become increasingly common for institutions to insure a very large segment of their employee base, including non-officers. Because non-MEC designs have a higher ratio of death benefit to premium dollar invested, some institutions have, therefore, taken out very high death benefit policies on employees, including lower-level employees, further adding to reputation risk and highlighting the importance of obtaining explicit consent.

Credit Risk

Credit risk is the potential impact on earnings and capital arising from an obligor's failure to meet the terms of any contract with the institution or otherwise perform as agreed. All life insurance policyholders are exposed to credit risk. The credit quality of the insurance company and duration of the contract are key variables. With insurance, credit risk arises from the insurance carrier's contractual obligation to pay death benefits upon the death of the insured, and if applicable, from the carrier's obligation to pay the CSV (less any applicable surrender charges) upon the surrender of the policy.

Most BOLI products have very long-term (30- to 40-year) expected time frames for full collection of cash proceeds, i.e., the death benefit. For general-account policies, the CSV is an unsecured, long-term, and nonamortizing obligation of the insurance carrier. Institutions record and carry this claim against the insurance company as an asset.

Before purchasing BOLI, an institution should conduct an independent financial analysis of the insurance company and continue to monitor its condition on an ongoing basis. The institution's credit-risk-management function should participate in the review and approval of insurance carriers. As with lending, the depth and frequency of credit analysis (both initially and on an ongoing basis) should be a function of the relative size and complexity of the transaction and the size of outstanding exposures. Among other things, an institution should consider its legal lending limit, concentration guidelines (generally defined as the aggregate of direct, indirect, and contingent obligations and exposures that exceed 25 percent of the institution's capital), and any applicable state restrictions on BOLI holdings when assessing its broader credit-risk exposure to insurance carriers. To measure

11. Mayo v. Hartford Life Insurance Company, 354 F.3d 400 (5th Cir. 2004).

credit exposures comprehensively, an institution should aggregate its exposures to individual insurance carriers, and the insurance industry as a whole, attributable to both BOLI policies and other credit relationships (e.g., loans and derivatives exposures).

There are product design features of a BOLI policy that can reduce credit risk. As noted earlier, an institution can purchase separate-account products, where the institution assumes the credit risk of the assets held in the separate account, rather than the direct credit risk of the carrier as would be the case in a general-account policy. With separate-account policies, the insurance carrier owns the assets, but maintains the assets beyond the reach of general creditors in the event of the insurer's insolvency. However, even with a separate-account policy, the policy owner incurs some general-account credit-risk exposure to the insurance carrier associated with the carrier's mortality and DAC reserves. Amounts equal to the mortality and DAC reserves are owed to the policyholder and represent general-account obligations of the insurance carrier. In addition, the difference, if any, between the CSV and the minimum guaranteed death benefit would be paid out of the insurance carrier's general account.

A separate-account policy may have a stable value protection (SVP) contract issued by the insurance carrier or by a third party that is intended to protect the policyholder from most declines in fair value of separate-account assets. In general, the provider of an SVP contract agrees to pay any shortfall between the fair value of the separate-account assets when the policy owner surrenders the policy and the cost basis of the separate account to the policy owner. Under most arrangements, the insurance carrier is not responsible for making a payment under the SVP contract if a third-party protection provider fails to make a required payment to it. The SVP contract thus represents an additional source of credit risk for a separate-account product. The policyholder's exposure under an SVP contract is to both the protection provider, which must make any required payment to the insurance carrier, and the carrier, which must remit the payment received from the protection provider to the institution. Because of this exposure, an institution should also evaluate the repayment capacity of the SVP provider.

State insurance regulation governing reserve requirements for insurance carriers, state guaranty funds, and reinsurance arrangements help to reduce direct credit risks from general-account exposures. Further, an institution can use a 1035 exchange to exit a deteriorating credit exposure, although most policies impose fees for the exchange. While credit risk for existing general- and separate-account policies may be low currently, the extremely long-term nature of a BOLI policy underscores the fact that credit risk remains an important risk associated with life insurance products. Strong current credit ratings offer no guarantee of strong credit ratings 20, 30, or 40 years into the future.

Interest-Rate Risk

Interest-rate risk is the risk to earnings and capital arising from movements in interest rates. Due to the interest-rate risk inherent in general-account products, it is particularly important that management fully understand how these products expose the policyholder to interest-rate risk before purchasing the policy. The interest-rate risk associated with these products is primarily a function of the maturities of the assets in the carrier's investment portfolio, which often range from four to eight years. When purchasing a general-account policy, an institution chooses one of a number of interest-crediting options (that is, the method by which the carrier will increase the policy's CSV). Using the "portfolio" crediting rate, the institution will earn a return based upon the existing yield of the carrier's portfolio each year. Using the "new money" crediting rate, the institution earns a return based upon yields available in the market at the time it purchases the policy.

Separate-account products may also expose the institution to interest-rate risk, depending on the types of assets held in the separate account. For example, if the separate-account assets consist solely of U.S. Treasury securities, the institution is exposed to interest-rate risk in the same way as holding U.S. Treasury securities directly in its investment portfolio. However, because the institution cannot control the separate-account assets, it is more difficult for the institution to control this risk. Accordingly, before purchasing a separate-account product, an institution's management should thoroughly review and understand the instruments governing the investment policy and management of the separate account. Management should understand the risk inherent within the separate account and

ensure that the risk is appropriate for the institution. The institution also should establish monitoring and reporting systems that will enable management to monitor and respond to interest-rate fluctuations and their effect on separate-account assets.

Compliance/Legal Risk

Compliance/legal risk is the risk to earnings and capital arising from violations of, or nonconformance with, laws, rulings, regulations, prescribed practices, or ethical standards. Failure to comply with applicable laws, rulings, regulations, and prescribed practices could compromise the success of a BOLI program and result in fines or penalties imposed by regulatory authorities or loss of tax benefits. Among the legal and regulatory considerations that an institution should evaluate are compliance with state insurable interest laws, the Employee Retirement Income Security Act of 1974 (ERISA), Federal Reserve Regulations O and W (12 CFR 215 and 223, respectively), the Interagency Guidelines Establishing Standards for Safety and Soundness, the requirements set forth under the "Legal Authority" section of this document, and federal tax regulations applicable to BOLI.

Tax benefits are critical to the success of most BOLI plans. Accordingly, an institution owning separate-account BOLI must implement internal policies and procedures to ensure that it does not take any action that might be interpreted as exercising "control" over separate-account assets. This is especially important for privately placed policies in which the institution is the only policyholder associated with the separate-account assets.

When purchasing BOLI, institutions should be aware that the splitting of commissions between a vendor and the institution's own subsidiary or affiliate insurance agency presents compliance risk. The laws of most states prohibit the payment of inducements or rebates to a person as an incentive for that person to purchase insurance. These laws may also apply to the person receiving the payment. When an insurance vendor splits its commission with an institution's insurance agency that was not otherwise involved in the transaction, such a payment may constitute a prohibited inducement or rebate. Accordingly, an institution should assure itself that this practice is permissible under applicable state law and in compliance with Federal Reserve Regulation W before participating in any such arrangement. Moreover, payments to an affiliate that did not perform services for the institution could also raise other regulatory and supervisory issues.

Due to the significance of the compliance risk, institutions should seek the advice of counsel on these legal and regulatory issues.

Price Risk

Price risk is the risk to earnings and capital arising from changes in the value of portfolios of financial instruments. Accounting rules permit owners of insurance contracts to account for general-account products using an approach that is essentially based on cost plus accrued earnings. However, for separate-account products without SVP, the accounting would largely be based on the fair value of the assets held in the account because this value is the amount that could be realized from the separate account if the policy is surrendered. (See "Accounting Considerations" above.) Typically, the policyholder of separate-account products assumes all price risk associated with the investments within the separate account. Usually, the insurance carrier will provide neither a minimum CSV nor a guaranteed interest-crediting rate for separate-account products. Absent an SVP contract, the amount of price risk generally depends upon the type of assets held in the separate account.

Because the institution does not control the separate-account assets, it is more difficult for it to control the price risk of these assets than if they were directly owned. To address income-statement volatility, an institution may purchase an SVP contract for its separate-account policy. The SVP contract is designed to ensure that the amount that an institution could realize from its separate-account policy, in most circumstances, remains at or above the cost basis of the separate account to the policyholder. Institutions should understand, however, that SVP contracts protect against declines in value attributable to changes in interest rates; they do not cover default risk. Moreover, one purpose of the SVP contract is to reduce volatility in an institution's reported earnings. To realize any economic benefit of the SVP contract, an institution would have to surrender the policy. Since policy surrender is nearly always an uneconomic decision, the SVP contract provides, in a practical sense, accounting benefits only.

Before purchasing a separate-account life insurance product, management should thoroughly review and understand the instruments governing the investment policy and management of the separate account. Management should understand the risk inherent in the separate account and ensure that the risk is appropriate. If the institution does not purchase SVP, management should establish monitoring and reporting systems that will enable it to recognize and respond to price fluctuations in the fair value of separate-account assets.

Under limited circumstances it is legally permissible for an institution to purchase an equity-linked variable life insurance policy if the policy is an effective economic hedge against the institution's equity-linked obligations under employee benefit plans.[12] An effective economic hedge exists when changes in the economic value of the liability or other risk exposure being hedged are matched by counterbalancing changes in the value of the hedging instrument. Such a relationship would exist where the obligation under an institution's deferred compensation plan is based upon the value of a stock market index and the separate account contains a stock mutual fund that mirrors the performance of that index. Institutions need to be aware that this economic hedge may not qualify as a hedge for accounting purposes. Thus, the use of equity-linked variable life insurance policies to economically hedge equity-linked obligations may not have a neutral effect on an institution's reported earnings.

Unlike separate-account holdings of debt securities, SVP contracts on separate-account equity holdings are not common. The economic hedging criteria for equity-linked insurance products lessen the effect of price risk because changes in the amount of the institution's equity-linked liability are required to offset changes in the value of the separate-account assets. If the insurance cannot be characterized as an effective economic hedge, the presence of equity securities in a separate account is impermissible, and the agencies will require institutions to reallocate the assets unless retention of the policy is permitted under federal law.[13]

In addition to the general considerations discussed previously, which are applicable to any separate-account product, an institution should perform further analysis when purchasing a separate-account product involving equity securities. At a minimum, the institution should:

1. Compare the equity-linked liability being hedged (e.g., deferred compensation) and the equity securities in the separate account. Such an analysis considers the correlation between the liability and the equity securities, expected returns for the securities (including standard deviation of returns), and current and projected asset and liability balances.
2. Determine a target range for the hedge effectiveness ratio (e.g., 95 to 105 percent) and establish a method for measuring hedge effectiveness on an ongoing basis. The institution should establish a process for altering the program if hedge effectiveness drops below acceptable levels. Consideration should be given to the potential costs of program changes.
3. Establish a process for analyzing and reporting to management and the board the effect of the hedge on the institution's earnings and capital ratios. The analysis usually considers results both with and without the hedging transaction.

Risk-Based Capital Treatment

If an institution owns a general-account insurance product, it should apply a 100 percent risk weight to its claim on the insurance company for risk-based capital purposes. A BOLI investment in a separate-account insurance product, however, may expose the institution to the market and credit risks associated with the pools of assets in the separate account. The assets in a pool may have different risk weights, similar to the assets held in a mutual fund in which an institution has invested. For risk-based capital purposes, if an institution can demonstrate that the BOLI separate-account policy meets the requirements below, it may choose to "look through" to the underlying assets to determine the risk weight.

12. Insured state banks and state savings associations may make such purchases only if permitted to do so under applicable state law.

13. Insured state banks and state savings associations may request the FDIC's consent to retain the policies, but consent will not be granted if it is determined that retaining the policies presents a significant risk to the appropriate insurance fund.

Criteria for a Look-Through Approach

To qualify for the "look-through" approach, separate-account BOLI assets must be protected from the insurance company's general creditors in the event of the insurer's insolvency. An institution should document its assessment, based upon applicable state insurance laws and other relevant factors, that the separate-account assets would be protected from the carrier's general creditors. If the institution does not have sufficient information to determine that a BOLI separate-account policy qualifies for the look-through approach, the institution must apply the standard risk weight of 100 percent to this asset.

In addition, when an institution has a separate-account policy, the portion of the carrying value of the institution's insurance asset that represents general-account claims on the insurer, such as deferred acquisition costs (DAC) and mortality reserves that are realizable as of the balance-sheet date, and any portion of the carrying value attributable to an SVP contract, are not eligible for the look-through approach. These amounts should be risk-weighted at the 100 percent risk weight applicable to claims on the insurer or the SVP provider, as appropriate.

Look-Through Approaches

When risk-weighting a qualifying separate-account policy, an institution may apply the highest risk weight for an asset permitted in theseparate account, as stated in the investment agreement, to the entire carrying value of the separate-account policy, except for any portions of the carrying value that are general-account claims or are attributable to SVP. In no case, however, may the risk weight for the carrying value of the policy (excluding any general-account and SVP portions) be less than 20 percent.

Alternatively, an institution may use a pro rata approach to risk-weighting the carrying value of a qualifying separate-account policy (excluding any general-account and SVP portions). The pro rata approach is based on the investment limits stated in the investment agreement for each class of assets that can be held in the separate account, with the constraint that the weighted average risk weight may not be less than 20 percent. If the sum of the permitted investments across market sectors in the investment agreement is greater than 100 percent, the institution must use the highest risk weight for the maximum amount permitted in that asset class, and then proceed to the next-highest risk weight until the permitted amounts equal 100 percent.

For example, if a separate-account investment agreement permits a maximum allocation of 60 percent for corporate bonds, 40 percent for U.S. government–sponsored enterprise debt securities, and 60 percent for U.S. Treasury securities, then the institution must risk-weight 60 percent of the carrying value of the separate-account investment (excluding any portion attributable to SVP) at the 100 percent risk weight applicable to corporate bonds and the remaining 40 percent at the 20 percent risk weight for U.S. government–sponsored enterprise debt securities. Because the sum of the permitted allocation for corporate bonds and government-sponsored enterprise debt securities totals 100 percent, the institution cannot use the zero percent risk weight for U.S. Treasury securities. However, if the permitted allocation for U.S. government–sponsored enterprise debt securities was 30 percent rather than 40 percent, the institution could risk-weight the remaining 10 percent of the carrying value of its investment at the zero percent risk weight for U.S. Treasuries.

Regardless of the look-through approach an institution employs, the weighted average risk weight for the separate-account policy (excluding any general-account and SVP portions) may not be less than 20 percent, even if all the assets in the separate account would otherwise qualifyfor a zero percent risk weight. Furthermore, the portion of the carrying value of the separate-account policy that represents general-account claims on the insurer, such as realizable DAC and mortality reserves, and any portion of the carrying value attributable to an SVP contract, should be risk-weighted at the risk weight applicable to the insurer or the SVP provider, as appropriate.

The following example demonstrates the appropriate risk-weight calculations for the pro rata approach, incorporating the components of a BOLI separate-account policy that includes general-account claims on the insurer as well as the investment allocations permitted for different asset classes in the separate-account investment agreement.

Example. The separate-account investment agreement requires the account to hold a minimum of

10 percent in U.S. Treasury obligations. It also imposes a maximum allocation of 50 percent in mortgage-backed securities issued by U.S. government–sponsored enterprises, and a maximum allocation of 50 percent in corporate bonds.

Assume that the portion of the carrying value of the separate-account policy attributable to realizable DAC and mortality reserves equals $10 and that the portion attributable to the SVP totals $10.

Carrying value of separate-account policy	$100.00
Less: Portion attributable to DAC and mortality reserves	10.00
Portion attributable to SVP	10.00
Net carrying value of separate-account policy available for pro rata	$ 80.00
Risk-weight calculation:	
U.S. Treasury @ 10% x $80 = $8 x 0% RW	0.00
Corporate bonds @ 50% x $80 = $40 x 100% RW	$ 40.00
GSE MBS @ 40% x $80 = $32 x 20% RW	6.40
Separate-account risk-weighted assets subject to pro rata	$ 46.40
Add back: DAC and mortality reserves = $10 x 100% RW	$ 10.00
Add back: SVP = $10 x 100% RW	10.00
General-account and SVP risk-weighted assets	$ 20.00
Total BOLI-related risk-weighted assets	$ 66.40

Summary

The purchase of BOLI can be an effective way for institutions to manage exposures arising from commitments to provide employee compensation and pre- and post-retirement benefits. Consistent with safe and sound banking practices, institutions must understand the risks associated with this product and implement a risk-management process that provides for the identification and control of such risks. A sound pre-purchase analysis, meaningful ongoing monitoring program, reliable accounting process, and accurate assessment of risk-based capital requirements are all components of the type of risk-management process the agencies expect institutions to employ.

Where an institution has acquired BOLI in an amount that approaches or exceeds agency concentration levels, examiners will more closely scrutinize the components of the risk-management process and the institution's associated documentation. Where BOLI has been purchased in an impermissible manner, ineffective controls over BOLI risks exist, or a BOLI exposure poses a safety-and-soundness concern, the appropriate agency may take supervisory action, including requiring the institution to divest affected policies, irrespective of tax consequences.

Appendix A—Common Types of Life Insurance

Life insurance can be categorized into two broad types: temporary (also called "term") insurance and permanent insurance. There are numerous variations of these products. However, most life insurance policies fall within one (or a combination) of the following categories.

Temporary (Term) Insurance

Temporary (term) insurance provides life insurance protection for a specified time period. Death benefits are payable only if the insured dies during the specified period. If a loss does not occur during the specified term, the policy

lapses and provides no further protection. Term insurance premiums do not have a savings component; thus, term insurance does not create cash surrender value (CSV).

Permanent Insurance

In contrast to term insurance, permanent insurance is intended to provide life insurance protection for the entire life of the insured, and its premium structure includes a savings component. Permanent insurance policy premiums typically have two components: the insurance component (e.g., mortality cost, administrative fees, and sales loads) and the savings component. Mortality cost represents the cost imposed on the policyholder by the insurance company to cover the amount of pure insurance protection for which the insurance company is at risk.

The savings component typically is referred to as CSV. The policyholder may use the CSV to make the minimum premium payments necessary to maintain the death benefit protection and may access the CSV by taking out loans or making partial surrenders. If permanent insurance is surrendered before death, surrender charges may be assessed against the CSV. Generally, surrender charges are assessed if the policy is surrendered within the first 10 to 15 years.

Two broad categories of permanent insurance are:

- *Whole life.* A traditional form of permanent insurance designed so that fixed premiums are paid for the entire life of the insured. Death benefit protection is provided for the entire life of the insured, assuming all premiums are paid.
- *Universal life.* A form of permanent insurance designed to provide flexibility in premium payments and death benefit protection. The policyholder can pay maximum premiums and maintain a very high CSV. Alternatively, the policyholder can make minimal payments in an amount just large enough to cover mortality and other insurance charges.

Purposes for Which Institutions Commonly Purchase Life Insurance

Key person. Institutions often purchase life insurance to protect against the loss of "key persons" whose services are essential to the continuing success of the institution and whose untimely death would be disruptive. For example, an institution may purchase insurance on the life of an employee or director whose death would be of such consequence to the institution as to give it an insurable interest in his or her life. The determination of whether an individual is a key person does not turn on that individual's status as an officer or director, but on the nature of the individual's economic contribution to the institution.

The first step in indemnifying an institution against the loss of a key person is to identify the key person. The next and possibly most difficult step is estimating the insurable value of the key person or the potential loss of income or other value that the institution may incur from the untimely death of that person.

Because the most appropriate method for determining the value of a key person is dependent upon individual circumstances, the agencies have not established a formula or a specific process for estimating the value of a key person. Instead, the agencies expect institutions to consider and analyze all relevant factors and use their judgment to make a decision about the value of key persons.

Key-person life insurance should not be used in place of, and does not diminish the need for, adequate management-succession planning. Indeed, if an institution has an adequate management-succession plan, its reliance on a key person should decline as the person gets closer to retirement.

Financing or cost recovery for benefit plans. Like other businesses, institutions often use life insurance as a financing or cost-recovery vehicle for pre- and post-retirement employee benefits, such as individual or group life insurance, health insurance, dental insurance, vision insurance, tuition reimbursement, deferred compensation, and pension benefits.

Permanent insurance is used for this purpose. In these arrangements, an institution insures the lives of directors or employees in whom it has an insurable interest to reimburse the institution for the cost of employee benefits. The group of insured individuals may be different from the group that receives benefits. The institution's obligation to provide employee benefits is separate and distinct from the purchase of the life insurance. The life insurance purchased by the institution remains an asset even after the

employer's relationship with an insured employee is terminated. The employees who receive benefits, whether insured or not, have no ownership interest in the insurance (other than their general claim against the institution's assets arising from the institution's obligation to provide the stated employee benefits).

There are two common methods of financing employee benefits through the purchase of life insurance. The first is the cost-recovery method, which usually involves present-value analysis. Typically, the institution projects the amount of the expected benefits owed to employees and then discounts this amount to determine the present value of the benefits. Then, the institution purchases a sufficient amount of life insurance on the lives of certain employees so that the gain (present value of the life insurance proceeds less the premium payments) from the insurance proceeds reimburses the institution for the benefit payments. Under this method, the institution absorbs the cost of providing the employee benefits and the cost of purchasing the life insurance. The institution holds the life insurance and collects the death benefit to reimburse the institution for the cost of the employee benefits and the insurance.

The second method of financing employee benefits is known as cost offset. With this method, the institution projects the annual employee benefit expense associated with the benefit plan. Then, the institution purchases life insurance on the lives of certain employees. The amount earned on the CSV each year should not exceed the annual benefit expense.

Split-dollar life insurance arrangements. Institutions sometimes use split-dollar life insurance arrangements to provide retirement benefits and death benefits to certain employees as part of their compensation. Under split-dollar arrangements, the employer and the employee share the rights to the policy's CSV and death benefits. The employer and the employee may also share premium payments. If the employer pays the entire premium, the employee may need to recognize taxable income each year in accordance with federal income tax regulations.

Split-dollar arrangements may be structured in a number of ways. The two most common types of split-dollar arrangements are:

- *Endorsement split-dollar.* The employer owns the policy and controls all rights of ownership. The employer provides the employee an endorsement of the portion of the death benefit specified in the plan agreement with the employee. The employee may designate a beneficiary for the designated portion of the death benefit. Under this arrangement, the employer typically holds the policy until the employee's death. At that time, the employee's beneficiary receives the designated portion of the death benefits, and the employer receives the remainder of the death benefits.
- *Collateral-assignment split-dollar.* The employee owns the policy and controls all rights of ownership. Under these arrangements, the employer usually pays the entire premium or a substantial part of the premium. The employee assigns a collateral interest in the policy to the employer that is equal to the employer's interest in the policy. The employer's interest in the policy is set forth in the split-dollar agreement between the employer and the employee. Upon retirement, the employee may have an option to buy the employer's interest in the insurance policy. This transfer of the employer's interest to the employee is typically referred to as a "roll-out." If a "roll-out" is not provided or exercised, the employer does not receive its interest in the policy until the employee's death.

Split-dollar life insurance is a very complex subject that can have unforeseen tax and legal consequences. Internal Revenue Service regulations issued in 2003[14] govern the taxation of split-dollar life insurance arrangements entered into or materially modified after September 17, 2003.[15] These rules provide less favorable tax treatment to split-dollar arrangements than existed previously. Institutions considering entering into a split-dollar life insurance arrangement should consult qualified tax, insurance, and legal advisers.

Life insurance on borrowers. State law generally recognizes that a lender has an insurable interest in the life of a borrower to the extent of the borrower's obligation to the lender. In some states, the lender's insurable interest may equal the borrower's obligation plus the cost of insurance and the time value of money. Institutions are permitted to protect themselves against the

14. 68 *Fed. Reg.* 54336 (Sept. 17, 2003), chiefly codified at 26 CFR 1.61-22 and 1.7872-15.

15. Split-dollar arrangements entered into prior to September 17, 2003, and not materially modified thereafter may be treated differently.

risk of loss from the death of a borrower. This protection may be provided through self-insurance, the purchase of debt-cancellation contracts, or by the purchase of life insurance policies on borrowers.

Institutions can take two approaches in purchasing life insurance on borrowers. First, an institution can purchase life insurance on an individual borrower for the purpose of protecting the institution specifically against loss arising from that borrower's death. Second, an institution may purchase life insurance on borrowers in a homogeneous group of loans employing a cost-recovery technique similar to that used in conjunction with employee benefit plans. Under this method, the institution insures the group of borrowers for the purpose of protecting the institution from loss arising from the death of any borrower in the homogeneous pool. Examples of homogeneous pools of loans include consumer loans that have distinctly similar characteristics, such as automobile loans, credit card loans, and residential real estate mortgages.

When purchasing insurance on an individual borrower, an institution should, given the facts and circumstances known at the time of the insurance purchase, make a reasonable effort to structure the insurance policy in a manner consistent with the expected repayment of the borrower's loan. To accomplish this, management should estimate the risk of loss over the life of the loan and match the anticipated insurance proceeds to the risk of loss. Generally, the risk of loss will be closely related to the outstanding principal of the debt. The insurance policy should be structured so that the expected insurance proceeds never substantially exceed the risk of loss.

When purchasing life insurance on borrowers in a homogeneous pool of loans, an institution's management should, given the facts and circumstances known at the time of the insurance purchase, make a reasonable effort to match the insurance proceeds on an aggregate basis to the total outstanding loan balances. If allowed by state law, institutions may match the insurance proceeds to the outstanding loan balances plus the cost of insurance on either a present-value or future-value basis. This relationship should be maintained throughout the duration of the program.

The purchase of life insurance on a borrower is not an appropriate mechanism for effecting a recovery on an obligation that has been charged off, or is expected to be charged off, for reasons other than the borrower's death. In the case of a charged-off loan, the purchase of life insurance on the borrower does not protect the institution from a risk of loss since the loss has already occurred. Therefore, the institution does not need to purchase insurance. Acquiring insurance that an institution does not need may subject the institution to unwarranted risks, which would be an unsafe and unsound banking practice. In the case of a loan that the institution expects to charge off for reasons other than the borrower's death, the risk of loss is so pronounced that the purchase of life insurance by the institution at that time would be purely speculative and an unsafe and unsound banking practice.

Internal Revenue Code section 264(f) disallows a portion of an institution's interest deduction for debt incurred to purchase life insurance on borrowers. Institutions considering the purchase of insurance on borrowers should consult their tax advisers to determine the economic viability of this strategy.

Life insurance as security for loans. Institutions sometimes take an interest in an existing life insurance policy as security for a loan. Institutions also make loans to individuals to purchase life insurance, taking a security interest in the policy, a practice known as "insurance-premium financing." As with any other type of lending, extensions of credit secured by life insurance should be made on terms that are consistent with safe and sound banking practices. For instance, the borrower should be obligated to repay the loan according to an appropriate amortization schedule.

Generally, an institution may not rely on its security interest in a life insurance policy to extend credit on terms that excuse the borrower from making interest and principal payments during the life of the borrower with the result that the institution is repaid only when the policy matures upon the death of the insured. Lending on such terms is generally speculative and an unsafe and unsound banking practice.

Institutions may acquire ownership of life insurance policies for debts previously contracted (DPC) by invoking their security interest in a policy after a borrower defaults. Consistent with safety and soundness, institutions should use their best efforts to surrender or otherwise dispose of permanent life insurance acquired for DPC at the earliest reasonable opportunity.[16] In

16. The OCC has generally directed national banks to

the case of temporary insurance acquired for DPC, retention until the next renewal date or the next premium date, whichever comes first, will be considered reasonable.

Appendix B—Glossary

Cash surrender value (CSV). The value available to the policyholder if the policy is surrendered. If no loans are outstanding, this amount is generally available in cash. If loans have been made, the amount available upon surrender is equal to the cash surrender value less the outstanding loan (including accrued interest).

Deferred acquisition costs (DAC). DAC represents the insurance carrier's up-front costs associated with issuing an insurance policy, including taxes and commissions and fees paid to agents for selling the policy. The carrier charges the policyholder for these costs. Carriers capitalize DAC and recover them in accordance with applicable tax law. As the carrier recovers DAC, it credits the amount to the policyholder.

Experience-rated pricing. A pricing method that bases prices for insurance products on the actual expenses and claims experience for the pool of individuals being insured.

General account. A design feature that is generally available to purchasers of whole or universal life insurance whereby the general assets of the insurance company support the policy's CSV.

Interest-crediting rate. The gross yield on the investment in the insurance policy, that is, the rate at which the cash value increases before considering any deductions for mortality cost, load charges, or other costs that are periodically charged against the policy's cash value.

There are a number of crediting rates, including "new money" and "portfolio." Using the "portfolio" crediting rate, the institution will earn a return based upon the existing yield of the insurance carrier's portfolio each year. Using the "new money" crediting rate, the institution will earn a return based upon yields available in the market at the time it purchases the policy.

Modified endowment contract (MEC). Type of policy that is defined in Internal Revenue Code section 7702A. A MEC generally involves the payment of a single premium at the inception of the contract; thus, it fails the so-called seven-pay test set forth in the statute. MECs are denied some of the favorable tax treatment usually accorded to life insurance. For example, most distributions, including loans, are treated as taxable income. An additional 10 percent penalty tax also is imposed on distributions in some circumstances. However, death benefits remain tax-free.

Mortality charge. The pure cost of the life insurance death benefit within a policy. It represents a cost to the purchaser and an income item to the carrier. Mortality charges retained by the insurance carrier are used to pay claims.

Mortality reserve. In separate-account products, the mortality reserve represents funds held by an insurance carrier outside of the separate account to provide for the payment of death benefits.

Non-MEC. An insurance contract that is not categorized as a MEC under Internal Revenue Code section 7702A.

Separate account. A separate account is a design feature that is generally available to purchasers of whole life or universal life whereby the policyholder's CSV is supported by assets segregated from the general assets of the carrier. Under such an arrangement, the policyholder neither owns the underlying separate account nor controls investment decisions (e.g., timing of investments or credit selection) in the underlying separate account that is created by the insurance carrier on its behalf. Nevertheless, the policyholder assumes all investment and price risk.

Seven-pay test. The seven-pay test is a test set forth in Internal Revenue Code section 7702A that determines whether or not a life insurance product is a MEC for federal tax purposes.

Split-dollar life insurance. A split-dollar life insurance arrangement splits the policy's premium and policy benefits between two parties, usually an employer and employee. The two parties may share the premium costs while the policy is in effect, pursuant to a prearranged contractual agreement. At the death of the

surrender or divest permanent life insurance acquired for DPC within 90 days of obtaining control of the policy.

insured or the termination of the agreement, the parties split the policy benefits or proceeds in accordance with their agreement.

Stable value protection (SVP) contracts. In general, an SVP contract pays the policy owner of a separate account any shortfall between the fair value of the separate-account assets when the policy owner surrenders the policy and the cost basis of the separate account to the policy owner. The cost basis of the separate account typically would take into account the fair value of the assets in the account when the policy was initially purchased, the initial fair value of assets added to the account thereafter, interest credited to the account, the amount of certain redemptions and withdrawals from the account, and credit losses incurred on separate-account assets. Thus, SVP contracts mitigate price risk. SVP contracts are most often used in connection with fixed-income investments.

1035 exchange. A tax-free replacement of an insurance policy for another contract covering the same person(s) in accordance with section 1035 of the Internal Revenue Code.

Variable life insurance. Variable life insurance policies are investment-oriented life insurance policies that provide a return linked to an underlying portfolio of securities. The portfolio typically is a group of mutual funds chosen by the insurer and housed in a separate account, with the policyholder given some discretion in choosing among the available investment options.

Appendix C—Interagency Interpretations of the Interagency Statement on the Purchase and Risk Management of Life Insurance

The federal banking and thrift agencies developed responses to questions regarding the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance. A summary of these interpretations is included below to provide clarification on a wide variety of matters pertaining to financial reporting, credit-exposure limits, concentration limits, and the appropriate methodologies to use for calculating the amount of insurance an institution may purchase.

Legal Authority—State and Federal Law

As a general matter, the ability of state-chartered banks to purchase insurance (including equity-linked variable life insurance) is governed by state law. Section 24 of the Federal Deposit Insurance Act (the FDI Act) generally requires insured state-chartered banks to obtain the consent of the Federal Deposit Insurance Corporation (FDIC) before engaging as principal in activities (including making investments) that are not permissible for a national bank. Some state bank regulatory agencies have issued their own BOLI guidance or directives for their respective state-chartered institutions. A state-chartered institution should follow any BOLI guidance or directive issued by its state supervisory authority that is more restrictive than the interagency statement. Generally, if state law or policy is less restrictive than the interagency statement, a state-chartered institution should follow the interagency statement. If federal law is less restrictive than state law, a state-chartered institution should follow the state law.

Permissibility of Equity-Linked Securities in Separate-Account BOLI

The interagency statement states that national banks and federal savings associations may hold equity-linked variable life insurance policies (that is, insurance policies with a return tied to the performance of a portfolio of equity securities held in a separate account of the insurance company) only in very limited circumstances. Similarly, state member banks may also hold equity-linked variable life insurance policies only in very limited circumstances. Because the range of instruments with equity-like characteristics varies significantly, the permissibility of each such instrument must be analyzed on a case-by-case basis. Furthermore, the agencies have significant concerns regarding whether an institution properly understands the complex risk profile that securities with "equity-like" characteristics often present. Some securities, even if legally permissible, may be inappropriate for the vast majority of financial institutions, whether held in an investment portfolio or a separate-account BOLI product. The agencies' April 1998 Supervisory Policy Statement on Investment Securities and End-User Derivatives

Activities provides guidance on the appropriateness of investments and risk-management expectations.

Senior Management and Board Oversight—Establishing BOLI Concentration Limits

Each institution should establish internal policies and procedures governing its BOLI holdings that limit the aggregate cash surrender value (CSV) of policies from any one insurance company as well as the aggregate CSV of policies from all insurance companies. The interagency statement is not intended to loosen the standards with respect to prior BOLI guidance. The agencies have rigorous expectations regarding the establishment of prudent limits and appropriate board and management oversight of the limit-setting process. Accordingly, exceptions will be subject to increased supervisory attention. The agencies continue to expect institutions to adopt per-carrier limits for BOLI, keeping in mind legal lending limits. Although the federal statutory and regulatory lending limits do not, as a general rule, impose a per-carrier legal constraint on BOLI because BOLI is not a loan, BOLI nevertheless does represent a long-term credit exposure. The agencies expect institutions to manage credit exposures in a prudent manner, irrespective of whether the exposure is subject to a statutory or regulatory limit. If an institution establishes an aggregate limit for BOLI based upon its applicable capital concentration threshold, it would seldom be prudent to have its per-carrier limit equal to the aggregate limit. Apart from credit considerations, it is also important to diversify BOLI exposures in order to control transaction risks that may be associated with an individual carrier's policies.

Per-Carrier Limits

Institutions should establish a per-carrier limit for separate-account policies. Diversification among carriers reduces transaction risks. Institutions should also explicitly consider whether it is appropriate to combine general- and separate-account exposures from the same carrier for purposes of measuring exposure against internal limits. The agencies believe that institutions, based upon their risk tolerance and understanding of insurance risks, should determine for themselves whether to combine such policies. In this regard, the agencies note that separate-account policies also present general-account credit exposures. For example, deferred acquisition costs (DAC) and mortality reserves associated with separate-account policies are general obligations of the insurance carrier. Moreover, when the death of an insured occurs, the difference between the death benefit amount and the cash surrender value comes from the carrier's general account. Finally, the actual credit exposure under a BOLI policy may be many times greater than the carrying value of the policy currently recorded on the institution's balance sheet, given the typical relationship between CSV and policy death benefits. Institutions should keep these factors in mind when evaluating whether and, if so, how to aggregate general- and separate-account exposures for purposes of monitoring compliance with internal limits.

Legal Limits and Concentrations

When establishing internal CSV limits, an institution should consider its legal lending limit, the capital concentration thresholds, and any applicable state restrictions on BOLI holdings. The following are the agencies' capital concentration definitions:

- The FDIC uses 25 percent of tier 1 capital to measure a capital concentration.
- The other agencies use tier 1 capital plus the allowance for loan and lease losses (ALLL).

A state-chartered institution should be guided by the more restrictive of the applicable state and federal limitations and thresholds. For example, if a state defines BOLI as an extension of credit subject to a statutory or regulatory lending limit, or otherwise imposes a per-carrier limit on BOLI, then institutions subject to that state's jurisdiction should ensure that their BOLI exposure to an individual carrier does not exceed the applicable state limit.

Permissibility of Holding Life Insurance on Former Employees and Former Key Persons

A well-managed institution adequately documents the purpose for which it is acquiring BOLI, as part of its pre-purchase analysis. When an institution purchases life insurance on a group of employees (whether it is a group policy or a series of individual policies) as a means to finance or recover the cost of employee benefits, and one or more of the insured employees is no longer employed by the bank, the insurance coverage may be retained by the institution provided—

- the application of the cost-recovery or cost-offset method (see "Quantifying the Amount of Insurance Appropriate for the Institution's Objectives" below) indicates that the amount of insurance held is not in excess of the amount required to recover or offset the cost of the institution's employee benefits,
- the policy is not specifically designated to cover only loss of income to the banking organization that may arise from the death of the employee,
- the coverage continues to qualify as an insurable interest under applicable state law, and
- the insurance asset continues to be a permissible holding under applicable state law for state-chartered institutions.

Additionally, if the policy no longer qualifies as insurance under the applicable state insurable-interest law, the policy may no longer be eligible for favorable tax treatment. These conditions apply to "benefits BOLI" despite the fact that the former employee was a "key person."

This is in contrast to true key-person insurance, in which the institution purchases life insurance on a key person in order to protect itself from financial loss in the event of that person's death. The interagency statement provides that a national bank or federal savings association may be required to surrender or otherwise dispose of key-person life insurance held on an individual who is no longer a key person because the institution will no longer suffer a financial loss from the death of that person. However, when an individual upon whom key-person life insurance has been held is no longer a key person, an institution may be able to recharacterize its objective for the insurance policy as recovery of the cost of providing employee benefits. In such cases, the institution must demonstrate, through appropriate analysis and quantification, that the insurance coverage satisfies the retention conditions, as set forth in the preceding paragraph. For a state-chartered institution, the recharacterization and retention of such key-person life insurance must be permissible under applicable state law. In circumstances where a national bank or federal savings association would be required to surrender or otherwise dispose of key-person life insurance, a state-chartered institution must also surrender or otherwise dispose of a key-person policy unless the retention of the policy is permitted under applicable state law and the institution obtains the FDIC's consent to continue to hold the policy under section 24 or section 28 of the FDI Act, as appropriate.

Quantifying the Amount of Insurance Appropriate for the Institution's Objectives

Institutions are responsible for ensuring that they do not purchase excessive amounts of insurance coverage on their employees relative to salaries paid and the costs of benefits to recover. Examiners will evaluate an institution's BOLI holdings and make a supervisory judgment as to whether insurance amounts on employees are so excessive as to constitute speculation or an unsafe or unsound practice on a case-by-case basis, as they do for other aspects of an institution's operations. Such an evaluation would be based on the totality of the circumstances.

Institutions may use either the cost-recovery or cost-offset method to quantify the amount of insurance permissible for purchase to finance or recover employee benefit costs. When using the cost-offset approach, an institution must ensure that the projected increase in CSV each year over the expected duration of the BOLI is less than or equal to the expected employee benefit expense for that year. When using the cost-recovery method, regardless of an institution's quantification method, management must be able to support, with objective evidence, the reasonableness of all assumptions used in determining the appropriate amount of insurance coverage needed, including the rationale for its discount rates (when the cost-recovery method is used) and cost projections.

Applicability of Prior Guidance for Split-Dollar Arrangements

The pre-purchase analysis guidance in the interagency statement applies to life insurance policies used in split-dollar arrangements that are acquired after December 7, 2004. The guidance concerning the ongoing risk management of life insurance after its purchase applies to life insurance policies, including those used in split-dollar arrangements, regardless of when acquired.

The FDIC's prior guidance on split-dollar arrangements, which was included in supervisory guidance on BOLI that was issued in 1993, has been superseded; until the issuance of the interagency statement, the FDIC had generally followed the Office of the Comptroller of the Currency's prior guidelines from 2000. Otherwise, the prior guidance issued by the agencies on split-dollar life insurance remains in effect. Each agency issued the interagency statement under its own bulletin, letter, or notice. For example, the Federal Reserve Board's issuance of the interagency statement is cross-referenced in SR-04-19, and the prior guidance on split-dollar life insurance arrangements is not superseded.

Accounting Considerations

An institution may purchase multiple permanent insurance policies from the same insurance carrier, with each policy having its own surrender charges. In some cases, the insurance carrier will issue a rider or other contractual provision stating that it will waive the surrender charges if all of the policies are surrendered at the same time. Because it is not known at any balance-sheet date whether one or more of the policies will be surrendered before the deaths of the insureds, the possibility that the institution will surrender all of these policies simultaneously and avoid the surrender charges is a gain contingency. This guidance should be applied to all insurance policies held by an institution regardless of when they were acquired. Therefore, an institution that has purchased BOLI is required to report the CSV on the bank's balance sheet net of the surrender charges (even if the policies have been in force for some time and the institution's auditors have not previously required reporting the CSV net of the surrender charges).

Based on the agencies' review of FASB Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance" (TB 85-4), including its appendix, the agencies believe that TB 85-4 is intended to be applied on a policy-by-policy basis. It, therefore, does not permit the aggregation of multiple separate policies for balance-sheet-measurement purposes. Accordingly, the agencies do not intend to defer to institutions or their auditors on this issue. As of the balance-sheet date, an institution should determine the amount that could be realized under each separate insurance policy on a stand-alone basis without regard to the existence of other insurance policies or riders covering multiple policies. If a single insurance policy covers more than one individual, the realizable amount of the entire policy should be determined. A single insurance policy covering multiple individuals should not be subdivided into hypothetical separate policies for each covered individual, even if the carrier reports CSVs for each covered individual.

If a change in an institution's accounting for its holdings of life insurance is necessary for regulatory reporting purposes, the institution should follow Accounting Principles Board Opinion No. 20, "Accounting Changes"(APB 20).[17] APB 20 defines various types of accounting changes and addresses the reporting of corrections of errors in previously issued financial statements. APB 20 states that "[e]rrors in financial statements result from mathematical mistakes, mistakes in the application of accounting principles, or oversight or misuse of facts that existed at the time the financial statements were prepared."

For regulatory reporting purposes, an institution must determine whether the reason for a change in its accounting for its holdings of life insurance meets the APB 20 definition of an accounting error. If the reason for the change meets this definition and the amount is material, the error should be reported as a prior-period adjustment in the institution's regulatory reports. Otherwise, the effect of the correction of the error should be reported in current earnings. If the effect of the correction of the error is material, the institution should also consult with its primary federal regulatory agency to deter-

17. Effective December 15, 2005, APB 20 will be replaced by FASB Statement No. 154, "Accounting Changes and Error Corrections—A replacement of APB Opinion No. 20 and FASB Statement No. 3."

mine whether any previously filed regulatory reports should be amended. For the Call Report, the institution should report the amount of the adjustment in Schedule RI-A, item 2, "Restatements due to corrections of material accounting errors and changes in accounting principles," with an explanation in Schedule RI-E, item 4. The effect of the correction of the error on income and expenses since the beginning of the period in which the correction of prior-period earnings is reported should be reflected in each affected income and expense account on a year-to-date basis in the Call Report Income Statement (Schedule RI), not as a direct adjustment to retained earnings.

Rate of Return to the Bank in Split-Dollar Insurance Arrangements

The agencies would consider the institution's economic interest in a split-dollar life insurance arrangement policy, at a minimum, to be a return of the premiums paid plus a reasonable rate of return. The agencies would generally consider a reasonable rate of return to be one that provides the bank a return that is commensurate with alternative investments having similar risk characteristics (including credit quality and term) at the time in which the bank enters into the split-dollar arrangement. The rate of return is to be calculated net of any payments made (or to be made) from insurance proceeds to the employee's beneficiaries.

The agencies look at the economic value of compensation arrangements when determining the reasonableness of split-dollar compensation, but the agencies do not rely solely on income tax rules for determining this economic value. Other factors that the agencies might consider include, but are not limited to, the benefit of a split-dollar arrangement to the employee as a percentage of salary and the expected length of time until the institution recovers its invested funds.

1. To determine the level and direction of risk that purchases and holdings of life insurance pose to the state member bank, and to recommend corrective action, as appropriate.
2. To perform—
   a. a risk assessment that summarizes the level of inherent risk by risk category, and
   b. an assessment of the adequacy of the board of directors' and management's oversight of the activity, including an assessment of the bank's internal control framework.
3. To ensure that the risk assessment considers a state member bank's purchase and risk management of its—
   a. broad bank-owned life insurance (BOLI) programs, in which life insurance is purchased on a group of employees to offset employee benefit programs and the bank is the beneficiary;
   b. split-dollar insurance arrangements for individual (usually senior-level) bank employees; and
   c. holdings of key-person insurance.
4. Recognizing that management may not be as familiar with insurance products as it is with more-traditional bank products, to adequately identify and assess the risks of BOLI, as well as the risk exposures that may arise from purchases and holdings of life insurance.[1]
5. To apply a forward-looking approach to the review of a bank's purchase and risk management of life insurance, recognizing that the bank may be exposed to increasing operational risks as a result of its large purchases or holdings of this product. These risks may arise from—
   a. separate-account assets that contain holdings of complex equity-linked notes and derivative products;
   b. the growing use of guaranteed minimum death benefits and other complex guarantee structures, which may increase the operational risk to banks purchasing significant amounts of life insurance; and
   c. the potential losses that could result from—
      - inadequate recordkeeping, which may be related to tracking the potentially large variety of contracts and agreements and the potentially large number of insured current and former employees covered by the contracts, and
      - a failure to ensure that contract agreements between the insurance company, the vendor(s), and the employees are properly executed and honored.

1. As noted in more depth in section 4042.1, the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance, these risks include operational, liquidity, credit, legal, and reputational risk. Operational risk arises in part from the vast array of new life insurance products and structures being offered and from the complexity of tax considerations related to the products, under various state insurable-interest and federal tax laws.

PRELIMINARY RISK ASSESSMENT

1. Consider the following, among other relevant criteria as appropriate, when determining whether to include the review of bank-owned life insurance (BOLI) in the examination scope:
   a. the volume, growth, and complexity of BOLI purchases and holdings
      - Consider the amount of the bank's BOLI holdings, measured by the total of their cash surrender values (CSVs) as a percentage of capital, and determine whether the resulting percentage is an asset concentration of capital. (For state member banks, the Federal Reserve has defined the capital base for determining this concentration threshold to be a percentage of tier 1 capital plus the allowance for loan and lease losses.) Determine whether the BOLI holdings have grown or declined significantly in recent years, when compared with the BOLI holdings of peer banks (consult the Federal Reserve System's intranet for applicable surveillance and monitoring data).
      - Obtain a breakout of the CSV of BOLI assets, as reported on the bank's balance sheet, including the amounts attributable to split-dollar insurance arrangements, general BOLI plans covering a group of employees to recover the cost of employee compensation and benefit programs, and the amount, if any, attributable to key-person insurance.
      - Obtain a listing of the amount of the bank's reimbursable premium payments under split-dollar life insurance arrangements and the amount receivable for these policies, which is to be booked as ''other assets'' on the bank's balance sheet.
      - Determine whether a portion of the CSV is in separate-account holdings of a life insurance company. If the bank has separate-account holdings, determine (1) the composition of the underlying separate-account assets and (2) if these assets constitute higher-risk investments, including equity-linked notes, mortgage-backed securities with significant interest-rate risk, or other investments entailing significant market risk.
      - Determine whether any of the life insurance policies are held in out-of-state trusts. If so, ascertain—
        — whether management and the board of directors can demonstrate that they have performed an independent legal analysis to ensure that the legal structure employed does not jeopardize the bank's insurable interest in the insurance policies or its access to the policy proceeds, as applicable; and
        — whether the trust arrangement inappropriately disadvantages the bank (for example, by permitting inappropriate investments or permitting the insured or the beneficiary to borrow against the policy holding in such a way that could jeopardize the bank's ability to recover amounts owed to it under the trust agreement).
   b. BOLI concentrations
      - Determine if there is a CSV concentration of life insurance to one carrier in excess of 25 percent that includes both separate-account and general-account BOLI holdings.
      - Determine if there are any market-risk concentrations within the underlying separate-account assets, including, for example, interest-sensitive fixed-income holdings.
      - Determine if there are any equity-linked notes or direct equity holdings in the separate accounts.
      - Determine if the bank holds any large-exposure life insurance policies on particular individuals. If so, determine if the policies are split-dollar arrangements and, if so—
        — whether the board or a board committee has evaluated the rea-

sonableness of the compensation as part of the employee's overall compensation package, and
— whether the board or a board committee has determined that the overall compensation is appropriate.

c. the appropriateness and recency of materials presented to the bank's board of directors concerning the bank's purchase and risk management of life insurance relative to its insurance purchases and holdings
d. the appropriateness and recency of audits and compliance reviews of the bank's purchases and risk management of life insurance
e. the overall financial condition of the bank, its supervisory rating, and any concerns or potential concerns about its liquidity

2. Depending upon the outcome of the preliminary risk assessment and other relevant factors, consider performing the following examination procedures.

OPERATIONAL-RISK ASSESSMENT

Senior Management and Board Oversight

1. Evaluate whether board and senior management oversight is effective and ensures that the bank's purchases and holdings of BOLI are consistent with safe and sound banking practices.
2. Determine whether the board of directors understands the complex risk characteristics of the bank's insurance holdings and the role of BOLI in the bank's overall business strategy.

Accounting Considerations

3. Determine if the bank's financial and regulatory reporting of its life insurance activities follows applicable generally accepted accounting principles (GAAP), including the following guidance:
   a. *Financial Accounting Standards Board (FASB) Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance" (TB 85-4).* Only the amount that can be realized under an insurance contract as of the balance-sheet date (that is, the CSV reported to the bank by the insurance carrier, less any applicable surrender charges not reflected by the insurance carrier in the reported CSV) is reported as an asset. Since there is no right of offset, a BOLI investment is reported as an asset separately from any deferred compensation liability, provided that it was not purchased in connection with a tax-qualified plan.
   b. *Call Report instructions.* The bank is required to report the carrying value of its BOLI holdings (CSV net of applicable surrender charges) as a component of "other assets" and to report the earnings on these holdings as "other noninterest income."
4. Verify that the bank's deferred compensation agreements were accounted for using the guidance in the February 11, 2004, Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance.
5. Verify that any accounts receivable that represent the bank's reimbursable life insurance premiums paid are recorded as unimpaired account receivables (for example, life insurance policies that are not impaired as a result of declining CSVs backing the obligations or employees borrowing against CSVs). (Impaired amounts should be expensed.)

Policies and Procedures

6. Assess the adequacy of the bank's policies and procedures governing its BOLI purchases and holdings, including its guidelines to limit the aggregate CSV of policies from one insurance company as well as limit the aggregate CSV of policies from all insurance companies.
7. Verify if the bank's board of directors or the board's designated committee approved BOLI purchases in excess of 25 percent of capital or in excess of any lower internal limit. (For state member banks, the Federal Reserve has defined the capital base for determining this concentration threshold to be a percentage of tier 1 capital plus the

allowance for loan and lease losses.)

8. Determine the reasonableness of the bank's internal limits and whether management and the board of directors have considered, before purchasing BOLI, the bank's legal lending limit, its applicable state and federal capital concentration threshold, and any other applicable state restrictions on BOLI.
9. For banks that may have other credit exposures to insurance companies, determine if the bank has considered the credit exposures arising from its BOLI purchases when assessing its overall credit exposure to a carrier and to the insurance industry.
10. Determine whether the bank's management has justified and analyzed the risks associated with a significant increase in the bank's BOLI holdings.
11. Determine if the bank has advised its board of directors of the existence of the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance and of the risks associated with BOLI.

Pre-Purchase Analysis

12. Ascertain whether the bank maintains adequate records of its pre-purchase analysis of BOLI.
13. Evaluate whether the bank's board of directors, or a designated board committee, and senior management understand the risks, rewards, and unique characteristics of BOLI.

Need for Insurance, Economic Benefits, and Appropriate Insurance Type

14. Determine whether the bank identified the specific risk of loss to which it is exposed or the specific costs to be recovered by the purchase of life insurance.
15. Determine whether the bank analyzed the costs and benefits of planned BOLI purchases.

Amount of Insurance Appropriate for the Institution's Objectives

16. Find out if the bank estimated the size of its employee benefit obligation or the risk of loss to be covered in order to ensure that the amount of BOLI purchased was not excessive in relation to this estimate and the associated product risks.
17. Determine whether management can support, with objective evidence, the reasonableness of all of the assumptions used in determining the appropriate amount of insurance coverage needed by the bank, including the rationale for its discount rates and cost projections.

Vendor Qualifications

18. Evaluate whether the bank's management assessed its own knowledge of insurance risks, the vendor's qualifications, the amount of resources the bank is willing to spend to administer and service the BOLI, and the vendor's ability to honor the long-term financial commitments associated with BOLI.

Characteristics of Available Insurance Products

19. Evaluate whether the bank's management has reviewed and understands the characteristics of the various life insurance products available and of the products it has acquired.
20. Ascertain if and how the bank's management reviewed and selected the life insurance product characteristics that best matched its objectives, needs, and risk tolerance. Ascertain whether management evaluated and documented, before the bank acquired BOLI, the risks of the variety and complexity of life insurance products considered, how the selected insurance product works, the variables that affect the product's performance, and the applicable tax and accounting treatments.
21. Determine whether the bank's management reviewed and documented its consideration of the types and design features of BOLI. Determine whether management reviewed and documented the negotiable features associated with a separate-account insurance product (for example, its investment options, terms, and conditions; the cost of stable value protection (SVP); deferred acquisition costs (DAC); and mortality options) and with any SVP provider that

may have been separately contracted by the insurance carrier.

22. Verify that the bank's management conducted a thorough review of life insurance policies before acquiring the policies. Ascertain if management determined how the accounting rules would apply to those policies and if it understood any ambiguous contract provisions, such as costs, charges, or reserves, that may affect the amount of a policy's CSV.

Tax and Insurable-Interest Implications

23. For the bank's pre-acquisition review of BOLI and its subsequent BOLI purchases, verify that the bank's management considered and documented its analysis of the financial impact of surrendering a policy (for example, any tax implications).
24. Verify that the bank's management obtained appropriate legal reviews. An appropriate legal review ensures that—
    a. the bank complies with applicable tax and state insurable-interest requirements, and
    b. the bank's insured amounts are *not* excessive (therefore, the bank is not involved in impermissible speculation or unsafe and unsound banking practices).

Carrier Selection

25. Find out if the bank (1) reviewed the BOLI product's design and pricing and the administrative services of the proposed carrier and (2) compared these services with those of other insurance carriers.
26. Ascertain whether the bank's management reviewed the selected carrier's ongoing long-term ability to commit to the BOLI product, as well as its credit ratings, general reputation, experience in the marketplace, and past performance.
27. Determine if the bank performed a credit analysis on the selected BOLI carriers and if the analysis was consistent with safe and sound banking practices for commercial lending.

Split-Dollar or Other Insurance Arrangements That Result in Additional Insured Employee Compensation

28. When a bank acquires insurance that permits a bank officer or employee to designate a beneficiary or provides the officer or employee with additional compensation, determine if the bank identified and quantified its total compensation objective. Determine if the bank ensured (1) that the acquired split-dollar life or other insurance arrangement was consistent with that objective, including when insurance compensation is combined with all other compensation being provided, and (2) that the total compensation was not excessive.
29. Verify that the bank and the insured have entered into a written agreement that specifically states the bank's rights, the insured individual's rights, and the rights of any other parties (trusts or beneficiaries) to the policy's CSV and death benefits.
30. Verify that the bank's shareholders and their family members (who are not bank officers, directors, or employees and who do not provide goods and services to the bank) do not receive compensation in the form of split-dollar life or other insurance coverage benefits.
31. Determine whether the bank's management has assessed the bank's ability to borrow against the CSV of its split-dollar life insurance policies, as well as the ability of other parties (whether an insured officer, employee, or noninstitution owner) to borrow against the policy CSV, without impairing the bank's financial interest in the policy proceeds. Determine also—
    a. if the bank can liquidate the policy in order to meet liquidity needs; or
    b. if the bank effects an early policy surrender (such as might occur if an employee terminates his or her employment), if the surrender would preclude the bank from recovering its premium payments and a market rate of return on the premiums invested.
32. Determine if and how management verified that the bank would be able to recover its premium payments plus a market rate of return on the premiums invested, after the payment of policy proceeds to the employee's beneficiary under the split-dollar arrangement.

Other Elements of Pre-Purchase Analysis

33. Ascertain whether the bank's management thoroughly evaluated all significant risks. Determine whether management has established procedures to identify, measure, monitor, and control those risks.
34. Find out if the bank, before acquiring BOLI, thoroughly analyzed its associated risks and benefits. As appropriate, determine whether the bank compared the risks of BOLI with those of alternative methods for recovering costs associated with the loss of key persons, providing pre- and post-retirement employee benefits, or providing additional employee compensation.

Post-Purchase Analysis

35. Find out if management reviewed at least annually the bank's life insurance purchases and holdings with the bank's board of directors.[1] Ascertain if the review included, at a minimum—
    a. a comprehensive assessment of the specific risks associated with the bank's permanent insurance acquisitions;
    b. an identification of the bank's employees who are or will be insured (for example, vice presidents and above, employees of a certain grade level, etc.);
    c. an assessment of death benefit amounts relative to employee salaries;
    d. a calculation of the percentage of insured persons still employed by the bank;
    e. an evaluation of the material changes to BOLI risk-management policies;
    f. an assessment of the effects of policy exchanges;
    g. an analysis of mortality performance and the impact on income;
    h. an evaluation of material findings from internal and external audits and independent risk-management reviews;
    i. an identification of the reason for, and the tax implications of, any policy surrenders; and
    j. a peer analysis of BOLI holdings.

LIQUIDITY-RISK ASSESSMENT

1. Find out if management, before the bank's purchase of permanent insurance, recognized the illiquid nature of the bank's acquisition of its permanent insurance products. Determine whether management ensured that the bank had the long-term financial flexibility to continue holding the insurance assets for their full term of expected use.
2. Determine if management, before the bank's purchase of permanent insurance, adequately considered the contractual arrangements and product types that limit product liquidity in order to best optimize the value of the bank's insurance assets and their possible future use as liquidity and funding sources. Contract provisions that should be considered include—
    a. 1035 exchange fees and "crawl-out restrictions,"
    b. provisions that would result in the product's categorization for federal tax purposes as a modified endowment contract (MEC) or a non-MEC contract, and
    c. SVP contract provisions that may limit the bank's ability to surrender a policy early or that would increase the cost of an early surrender.

REPUTATION-RISK ASSESSMENT

1. Ascertain whether the bank has taken steps, including obtaining written consent from its insured officers and employees, to reduce its reputation risk that may result from BOLI purchases.
2. Determine if the bank maintains appropriate documentation evidencing that it obtained a formal written consent from its insured officers and employees.
3. Find out what segment of the employee base the bank has insured (i.e., officers or non-officers) and if the bank has taken out very high death benefit policies on employees, including lower-level employees.

CREDIT-RISK ASSESSMENT

1. Determine if the bank's management con-

1. More-frequent reviews should be conducted if significant changes to the BOLI program are anticipated, such as additional purchases, a decline in the financial condition of the insurance carrier(s), anticipated policy surrenders, or changes in tax laws or interpretations that could have an impact on the performance of BOLI.

ducted an independent financial analysis of the insurance carrier before the bank's purchase of a life insurance policy.
   a. Ascertain if management continues to monitor the life insurance company's condition on an ongoing basis.
   b. Verify that the bank's credit-risk management function participated in the review and approval of insurance carriers.
2. Determine whether the bank considered its legal lending limit, its credit concentration guidelines (the aggregate exposures to individual insurance carriers and the life insurance industry, including other bank credit relationships, such as credit exposures involving loans and derivatives), and any state restrictions on BOLI holdings.
3. Determine whether the bank's credit analysis of its BOLI holdings evaluated whether the policies to be acquired were either separate-account or general-account policies.
   a. Find out whether the separate-account policies included an SVP contract to protect the bank (as a policyholder) from declines in the fair value of separate-account assets.
   b. Ascertain if the bank evaluated the insurance carrier's separately contracted SVP provider's repayment capacity.

MARKET-RISK ASSESSMENT

1. Determine whether management fully understood (before the bank purchased its separate-account products)—
   a. how the life insurance products expose the bank to interest-rate risk;
   b. the instruments governing the investment policy, as well as how the separate account is managed;
   c. the inherent risk of a separate account; and
   d. whether the bank's risk from the purchase of separate-account products was appropriate.
2. For general-account products, ascertain if management understands the interest-crediting option the bank chose when purchasing the insurance policy.
3. Find out if the bank has established and if it maintains appropriate monitoring and reporting systems for interest-rate fluctuations and their effect on separate-account assets.
4. Find out if the bank has acquired an SVP contract for its separate-account policy in order to reduce income-statement volatility. (SVP contracts protect against declines in value attributable to changes in interest rates; they do not cover default risk.)
5. If the bank has not purchased an SVP contract, determine if management has established and maintained monitoring and reporting systems that will recognize and respond to price fluctuations in the fair value of separate-account assets.
6. If the bank has purchased an equity-linked variable life insurance policy, determine whether it is characterized as an effective economic hedge against the bank's equity-linked obligations under its employee benefit plans. (An effective hedge exists when changes in the economic value of the liability or other risk exposure being hedged are matched by counterbalancing changes in the value of the hedging instruments. The economic hedging criteria for equity-linked insurance products lessen the effect of price risk because changes in the amount of the equity-linked liability are required to offset changes in the value of the separate-account assets.)
7. If the bank is purchasing or has purchased a separate-account insurance product involving equity securities, determine if the bank's management has performed further analysis that—
   a. compares the equity-linked liability being hedged and the equity securities in the separate account,
   b. determines a target range for the hedge-effectiveness ratio and establishes a method for measuring ongoing hedge effectiveness, and
   c. establishes a process for analyzing and reporting to management and the board of directors the effect of the hedge on the bank's earnings and capital ratios (both with and without the hedging transaction).

COMPLIANCE/LEGAL-RISK ASSESSMENT

1. Determine whether the bank's compliance

and audit functions have evaluated its compliance with applicable state insurable-interest and federal tax laws in order to protect the bank's earnings and capital from the loss of tax benefits or from the imposition of fines or penalties by regulatory authorities for violations of, or noncompliance with, laws, rulings, regulations, prescribed practices, and ethical standards.

2. When the bank owns separate-account BOLI, determine whether the bank has implemented and maintains internal control policies and procedures that adequately ensure that it does not take any action that might be interpreted as exercising ''control'' over separate-account assets.
3. Determine whether the bank split commissions between a vendor and the bank's own subsidiary or affiliate insurance agency when purchasing life insurance. If so, determine whether the bank's compliance function has assessed the bank's compliance with state and federal securities and insurance laws regarding fee and commission arrangements.
4. Ascertain whether the bank seeks and documents the advice of legal counsel when determining legal and regulatory issues, requirements, and concerns related to its potential purchase or ownership of BOLI.
5. For a general-account insurance product, determine if the bank has assigned a standard risk weight of 100 percent to the general-account asset.
6. For a BOLI separate-account product (when the bank uses the look-through approach to assign risk weights according to the risk-based capital rules)—
   a. review the bank's documentation, and determine if the bank adequately verified that the separate-account BOLI assets are protected from the insurance company's general creditors in the event of the insurance company's insolvency;
   b. determine if the standard risk weight of 100 percent was assigned to the bank's BOLI assets when the bank's documentation is inadequate or does not exist;
   c. verify that a 100 percent risk weight has been assigned to (1) the portion of the bank's insurance asset that represents general-account claims on the insurer (such as DAC and mortality reserves that are realizable on the balance-sheet date) and (2) any portion of the carrying value attributable to an SVP contract (or if the SVP provider is not an insurance company, verify that the correct risk weight has been assigned for that obligor); and
   d. if the bank used a pro rata approach to risk-weighting the carrying value of a qualifying separate-account policy—
      - verify that the risk weight is applied to the separate account based on the most risky portfolio that could be held by the separate account (as stated in the investment agreement), except for any portions of the carrying value that are general-account claims attributable to either DAC or an SVP (which are generally risk-weighted at 100 percent);
      - verify that in no case may the assigned risk weight for the bank's entire separate-account holding be less than 20 percent; and
      - when the sum of the permitted investments across market sectors in the investment agreement is greater than 100 percent, determine if the bank assigned the highest risk weight for the maximum amount permitted in that asset class, and then applied the next-highest risk weights to the other asset classes until the aggregate of the permitted amounts equals 100 percent.

Examiners should use only those internal control questions that are appropriate, given the size, complexity, and growth of a bank's bank-owned life insurance (BOLI) holdings.

PRELIMINARY RISK ASSESSMENT

1. Have the steps for conducting a preliminary risk assessment been followed, as they are set forth in section 4042.3? Have other relevant factors been considered to determine if further examination review may be warranted, in accordance with risk-focused supervision guidelines?
2. What particular factors have been identified to warrant a review of the bank's purchases and risk management of life insurance?

OPERATIONAL-RISK ASSESSMENT

Senior Management and Board of Directors Oversight

1. Has senior management and the board of directors initiated and maintained effective oversight of the bank's BOLI by—
   a. performing a thorough pre-purchase analysis of its risks and rewards and a post-purchase risk assessment?
   b. determining the permissibility of the bank's BOLI purchases and holdings under both the applicable state and federal requirements (whichever requirements are more restrictive)?
   c. determining the types and kinds of risks that are associated with BOLI?
   d. ascertaining and reviewing the safety-and-soundness considerations associated with the bank's BOLI?
   e. understanding the complex risk characteristics of the bank's insurance holdings and what role BOLI is to play in the bank's overall business?
2. Does the bank have a comprehensive risk-management process for purchasing and holding BOLI?

Accounting Considerations

3. When accounting for its holdings of life insurance, did the bank follow the guidance in FASB's Technical Bulletin No. 85-4, "Accounting for Purchases of Life Insurance"? Are the bank's insurance policies reported on its balance sheet on the basis of each policy's cash surrender value (CSV), less any applicable surrender charges that are not reflected in the reported CSV?
4. On the bank's Call Report, did the bank's management —
   a. report the carrying value of its BOLI holdings as an "other asset"?
   b. report the earnings on the bank's holdings as "other noninterest income"?
   c. report the CSV separately, as required if the CSV amount exceeded the reporting threshold?
   d. expense only the noninvestment portion of the premium, in the case of bank-owned policies?
   e. expense the premium for employee-owned insurance purchased by the bank and record a receivable in "other assets" for any portion of the premium to be reimbursed to the bank under a contractual agreement?
5. Were the bank's deferred compensation agreements accounted for using the guidance in the February 11, 2004, Interagency Advisory on Accounting for Deferred Compensation Agreements and Bank-Owned Life Insurance?

Policies and Procedures

6. Does the bank have comprehensive policies and procedures, including guidelines, that limit the aggregate CSV of policies from any one insurance company, as well as the aggregate CSV of policies from all insurance companies?
   a. Does the board of directors or a designated board committee require senior management to provide adequate and appropriate justification for establishing or revising internal CSV limits on the amount of BOLI the bank holds? Does

this justification take into account the bank's legal lending limits, its capital and credit concentration threshold, and any applicable laws and regulations?

b. Is written justification required when the amount of the bank's BOLI holdings approaches or exceeds 25 percent of the bank's capital (tier 1 capital plus the allowance for loan and lease losses)? Does the board of directors or a board committee approve this justification?

Pre-Purchase Analysis

7. Did the bank's management perform a written pre-purchase analysis of its BOLI products?
8. Did management identify the bank's need for BOLI, the appropriate type of insurance to be acquired, and the economic benefits to be derived from the purchase of BOLI? Did this analysis accomplish the following:
   a. identify the specific risk of loss to be covered by the insurance, or the costs the insurance is supposed to cover?
   b. determine what type BOLI (for example, general- or separate-account) and what BOLI features are needed, before acquiring the product?
   c. evaluate the permissibility and market risk of any underlying separate-account asset holdings, if separate-account BOLI is held?
   d. analyze projected policy values (CSV and death benefits) using various interest-crediting rates and mortality cost assumptions?
   e. estimate the size of the employee benefit obligation or the risk of loss to be covered? Did management ensure that the amount of BOLI coverage was appropriate for the bank's objectives and that BOLI was not excessive in relation to this estimate and the associated product risks?
   f. review the range of assumptions? Was management able to justify the assumptions with objective evidence, and deem them reasonable in view of previous and expected market conditions?
   g. assess whether the present value of the BOLI's expected future cash flows (net of the costs of the insurance) is less than the estimated present value of the expected after-tax employee benefit costs, when the bank uses BOLI to recover the costs of providing employee benefits?
9. Did the bank's management —
   a. review and assess its own knowledge of insurance risks, the vendor's qualifications, and the amount of the bank's resources that will be needed to administer and service the BOLI?
   b. demonstrate its familiarity with the technical details of the bank's insurance assets, and is management able to explain the reasons for and the risks associated with the product design features that have been selected?
   c. make appropriate inquiries to determine whether the vendor has the financial ability to honor its long-term commitments over an extended period of time?
   d. assure itself of the vendor's commitment to investing in the operational infrastructure that is necessary to support the BOLI?
   e. undertake its own independent review and not rely solely on prepackaged, vendor-supplied compliance information (such reliance is a potential cause for supervisory action)?
   f. properly evaluate the characteristics of the available insurance products against the bank's objectives, needs, and risk tolerance?
   g. determine if the bank's need for insurance on key persons or on a borrower's loan resulted in a matching of the maturity of the term or declining term insurance to the key person's expected tenure or the maturity of the borrower's loan?
   h. conduct a review of the insurance carrier that included—
      - a credit analysis of the potential insurance carrier (the analysis should have been performed in a manner consistent with safe and sound banking practices for commercial lending)?
      - a review of the bank's needs and a comparison of those needs with the proposed carrier's product design, pricing, and administrative services?
      - a review of the insurance carrier's commitment to the BOLI product, as well as the carrier's general reputation, experience in the marketplace, and past performance?

i. determine whether the total amount of compensation and insurance to be provided to an employee is excessive, if the purchased BOLI will result in the payment of additional compensation?
j. analyze the associated significant credit risks and the bank's ability to monitor and respond to those risks?
k. as appropriate, analyze the risks and benefits of BOLI, compared with other available methods for recovering costs associated with the loss of key persons, providing pre- and post-retirement employee benefits, or providing additional employee compensation?
l. sufficiently document its comprehensive pre-purchase analysis (including its analysis of both the types and product designs of purchased BOLI and the bank's overall level of BOLI holdings)?

Post-Purchase Analysis

10. Do management and the board of directors annually review the performance of the bank's insurance assets? Does the annual review include—
    a. a comprehensive assessment of the specific risks associated with permanent insurance acquisitions?
    b. an identification of employees who are or will be insured (e.g., vice presidents and above, employees of a certain grade level)?
    c. an assessment of death benefit amounts relative to employee salaries?
    d. a calculation of the percentage of insured persons still employed by the institution?
    e. an evaluation of the material changes to BOLI risk-management policies?
    f. an assessment of the effects of policy exchanges?
    g. an analysis of mortality performance and the impact on income?
    h. an evaluation of material findings from internal and external audits and independent risk-management reviews?
    i. an identification of the reason for and the tax implications of any policy surrenders?
    j. a peer analysis of BOLI holdings?

Tax and Insurable-Interest Implications

11. Has the bank's management explicitly considered the financial impact (for example, the tax provisions and penalties) of surrendering a BOLI policy?
12. Does the bank's management have or has it obtained appropriate legal review to ensure that it will be in compliance with applicable tax and state insurable-interest requirements? Is management aware of the relevant tax features of the insurance assets, including whether the bank's purchase would—
    a. make the bank subject to the alternative minimum tax?
    b. jeopardize the tax-advantaged status of the bank's insurance holdings?
    c. qualify (under applicable state law) an insurable ownership interest in the BOLI policy covering the bank's officers or its employees (including any applicable state law pertaining to the insured's consent and the amounts of allowable insurance coverage for an employee)?
13. Did the bank establish an out-of-state trust to hold its BOLI assets, and, if so, has the bank adequately assessed its insurable interest, given the arrangement?

LIQUIDITY-RISK ASSESSMENT

1. Has the bank's management fully recognized and considered the illiquid nature of the BOLI to be acquired? (An institution's BOLI holdings should be considered when assessing liquidity and assigning the component rating for liquidity.)
2. Did management determine if the bank has the long-term financial flexibility to hold the insurance asset for the full term of its expected use?

REPUTATION-RISK ASSESSMENT

1. Has the bank's management implemented procedures to ensure that the bank maintains appropriate documentation that evidences employees' informed consent for the bank's purchase of insurance on their lives? Do these procedures ensure that the bank

obtains employees' explicit consent before purchasing the insurance?

2. Has the bank obtained insurance products that insure large segments of its employee base (including the bank's non-officers)? Do these policies provide very high death benefits on employees, possibly causing the bank to be exposed to increased reputation risk if explicit consent was not obtained from the employees?

CREDIT-RISK ASSESSMENT

1. Did the bank's management conduct an independent financial analysis of the insurance carrier before purchasing the life insurance policy?
   a. Does management continue to monitor the life insurance company's financial condition on an ongoing basis?
   b. Did the bank's credit-risk management function participate in the review and approval of insurance carriers?
2. When establishing exposure limits for aggregate BOLI holdings and exposures to individual carriers, did the bank's management consider—
   a. the bank's legal lending limit?
   b. the applicable state and federal credit concentration exposure guidelines?
   c. the aggregate CSV exposures as a percentage of the bank's capital?
3. Has the bank's credit-risk management process taken into account credit exposures arising from both BOLI holdings and other credit exposures (loans, derivatives, and other insurance products) when measuring exposures to individual carriers?
4. Did the bank's credit analysis of its BOLI holdings consider whether the policies to be acquired were separate-account or general-account policies?
   a. For the separate-account policies, did the credit review include a risk analysis of the underlying separate-account assets?
   b. For separate-account policies that include a stable value protection (SVP) contract, has the repayment capacity of the insurance carrier's separately contracted SVP providers been evaluated?

MARKET-RISK ASSESSMENT

1. Did management adequately assess the interest-rate risk exposure of BOLI before purchasing the products for separate-account and general-account assets?
2. Has the bank's management reviewed, and does it understand the instruments governing the separate-account investment policy and its management?
   a. Does the bank's management understand the risk inherent within the separate account?
   b. Has the bank's management determined if the risk is appropriate?
3. Have monitoring and reporting systems been established that will enable the bank's management to monitor, measure, and appropriately manage interest-rate risk exposure from BOLI holdings when assessing the bank's overall sensitivity to interest-rate risk?

COMPLIANCE/LEGAL-RISK ASSESSMENT

1. Has the bank's audit and/or compliance function reviewed the bank's legal and regulatory requirements as they pertain to life insurance holdings? Did the review consider—
   a. state insurable-interest laws?
   b. the Employee Retirement Income Security Act of 1974 (ERISA)?
   c. the Federal Reserve Board's Regulation W (12 CFR 223)?
   d. applicable federal prohibitions on insider loans, including the Federal Reserve Board's Regulation O, that may apply to split-dollar life insurance arrangements?
   e. the interagency guidelines for establishing standards for safety and soundness?[1]
   f. other state and federal regulations applicable to BOLI?
2. To ensure that the life insurance qualifies for its tax-advantaged status, has the bank's management implemented and maintained internal policies and procedures to ensure that "control" will not be exercised over any of the separate-account assets, espe-

1. For state member banks, see 12 CFR 208, appendix D-1.

cially those involving privately placed policies?

3. Does the bank's board of directors, its designated board committee, and its management seek the assistance of legal counsel when determining the legal and regulatory issues related to the acquisition and holding of life insurance policies?
4. Has management thoroughly reviewed, and does it understand, the instruments governing the investment policy and the management of a separate account, before purchasing a separate-account policy?
5. If the bank has not purchased SVP for a separate-account BOLI policy, has management established the appropriate monitoring and reporting systems that will enable it to recognize and respond to price fluctuations in the fair value of the separate-account assets?
6. When the bank considers or purchases a separate-account BOLI product involving equity securities, does it analyze the equity securities? Does this analysis—
   a. compare the specific equity-linked liability being hedged against the securities held in a separate account?
   b. establish a target ratio for hedge effectiveness, as well as a method for measuring hedge effectiveness on an ongoing basis?
   c. establish a process for analyzing and reporting to the board of directors, its designated committee, and senior management the effect of the hedge on the bank's earnings and capital ratios (this analysis should include a consideration of the results both with and without the hedging transaction)?
7. When reporting its risk-based capital, has the bank ensured that it accurately calculates and reports its risk-weighted assets for BOLI holdings according to the risk-based capital guidelines and the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance (see section 4042.1 and SR-04-19 and its attachment)?
   a. For a general-account insurance product, has the bank applied a standard risk weight of 100 percent to the general-account asset?
   b. When the bank has applied a look-through approach for separate-account holdings—
      - has management determined if BOLI assets would be protected from the insurance company's general creditors in the event of its insolvency? Has the bank documented its assessment that BOLI assets are protected?
      - has the portion of the carrying value of the separate-account policy (that reflects the amounts attributable to the insurer's DAC and mortality reserves, and any other portion that is attributable to the carrying value of an SVP contract) been risk-weighted using the 100 percent risk weight applicable to the insurer's general-account obligations? Or, if the SVP provider is not an insurance company, has the portion of the carrying value been risk-weighted as appropriate for that obligor?
8. When the bank has used a pro rata approach to risk-weighting the carrying value of a qualifying separate-account policy, did it use the appropriate procedures, as outlined in the December 7, 2004, Interagency Statement on the Purchase and Risk Management of Life Insurance (see section 4042.1 and SR-04-19 and its attachment)?
   a. Has the bank ensured that its assigned aggregate risk weight for all separate-account BOLI holdings will be 20 percent or more?
   b. When the sum of the permitted investments across market sectors in the investment agreement is greater than 100 percent, was the highest risk weight applied for the maximum amount permitted in that asset class, and was the next-highest risk weight then applied until the cumulative permitted amounts equal 100 percent?

Banking organizations have long been engaged in the sale of insurance products and annuities, although these activities historically have been subject to several restrictions. For example, until recently, national banks could sell most types of insurance, but only through an agency located in a small town. Bank holding companies also were permitted to engage in only limited insurance agency activities under the Bank Holding Company Act. State-chartered banks, on the other hand, generally have been permitted to engage in insurance sales activities as agents to the extent permitted by state law.

The Gramm-Leach-Bliley Act of 1999 (the GLB Act), however, authorized national banks and state-chartered member banks to sell all types of insurance products through a financial subsidiary. *The GLB Act generally did not change the powers of banks to sell insurance directly.* As a result of the GLB Act and marketplace developments, many banking organizations are increasing the range and volume of their insurance and annuities sales activities. To the extent permitted by applicable law, banking organizations may conduct insurance and annuity sales activities through a variety of structures and delivery channels, including ownership of an insurance underwriter or an insurance agency or broker, the employment by a bank of licensed agents, a joint marketing arrangement with a producer,[1] independent agents located at a bank's office, direct mail, telemarketing, and Internet marketing.

A banking organization may also conduct insurance or annuity sales activities through a managing general agent (MGA). An MGA is a wholesaler of insurance products and services to insurance agents. The MGA has a contractual agreement with an insurance carrier to assume functions for the carrier, which may include marketing, accounting, data processing, policy recordkeeping, and monitoring or processing claims. The MGA may rely on various local agents or agencies to sell the carrier's products. Most states require an MGA to be licensed.

OVERVIEW AND SCOPE

The following guidance pertains to state member banks that are either directly or indirectly engaged in the sale of insurance or annuity products. Examiner guidance on performing appropriate risk assessments of a state member bank's insurance and annuity sales activities is included.[2] Additionally, guidance is provided for examining a state member bank's compliance with the consumer protection rules relating to insurance and annuities sales activities that are contained in the Board's December 2000 revisions to Regulation H (subpart H) (12 CFR 208.81–86), "Consumer Protection in Sales of Insurance" (CPSI). Subpart H, which became effective on October 1, 2001, implements the consumer protection requirements of the GLB Act, which are codified at 12 USC 1831x. (See 65 *Fed. Reg.* 75841, December 4, 2000.) The regulation applies not only to the sale of insurance products or annuities by the bank, but also to activities of any person engaged in insurance product or annuity sales on behalf of the bank, as discussed in this guidance. The guidance is generally not applicable to debt-cancellation contracts and debt-suspension agreements, unless these products are considered to be insurance products by the state in which the sales activities are conducted.

The GLB Act permits state member banks that are not authorized by applicable state law to sell insurance directly to do so through a financial subsidiary.[3] A financial subsidiary engaged in insurance sales may be located wherever state law permits the establishment and operation of

1. The term "producer" refers broadly to persons, partnerships, associations, limited liability corporations, etc., that hold a license to sell or solicit contracts of insurance to the public. Insurance agents and agencies are producers who, through a written contractual arrangement known as a direct appointment, represent one or more insurance underwriters. Independent agents and agencies are those producers that sell products underwritten by one or more insurance underwriters. Captive agents and agencies represent a specific underwriter and sell only its products. Brokers are producers that represent the purchaser of insurance and obtain bids from competing underwriters on behalf of their clients. State insurance laws and regulations often distinguish between an insurance agent and a broker; in practice, the terms are often used interchangeably.

2. The term "risk assessment" entails an analysis of (1) the level of inherent risk by type of risk (operational, legal, market, liquidity, and credit risk) for a business line or business function, (2) the adequacy of management controls over that business line or business function, and (3) the direction of the risk (increasing, decreasing, or stable).

3. Rules pertaining to state member bank financial subsidiaries are found in the Board's Regulation H (12 CFR 208.71–77).

an insurance agency. Such subsidiaries, however, would be subject to state licensing and other requirements.

The Federal Reserve is responsible for evaluating the consolidated risk profile of a state member bank. This reponsibility includes determining the risks posed to the state member bank from the insurance and annuity sales activities it conducts directly or indirectly, as well as determining the effectiveness of the bank's risk-management systems. However, the GLB Act also established a regulatory framework that is designed to ensure that the Federal Reserve coordinates with, and relies to the extent possible on information from, the state insurance authorities when it is supervising the insurance activities a state member bank conducts through a functionally regulated subsidiary.

Consistent with the Federal Reserve's risk-focused framework for supervising banking organizations, resources allocated to the review of insurance sales activities should be commensurate with the significance of the activities and the risk they pose to the bank. The scope of the review depends on the significance of the activity to the state member bank and the extent to which the bank is directly involved in the activity. Examiner judgment is required to tailor the reviews, as appropriate, on the basis of the legal, organizational, and risk-management structure of the state member bank's insurance and annuity sales activities and on other relevant factors.[4]

SUPERVISORY APPROACH FOR THE REVIEW OF INSURANCE AND ANNUITY SALES ACTIVITIES

Supervisory Objective

The primary objective for the review of a state member bank's insurance and annuity sales activities is to determine the level and direction of risk such activities pose to the state member bank. The review includes insurance and annuity sales activities the state member bank conducts directly (by or in conjunction with a subsidiary or affiliate) or through a third-party arrangement. Primary risks that may arise from insurance sales activities include operational and legal risk. If the state member bank does not adequately manage these risks, they could have an adverse impact on its earnings and capital. The examiner should produce (1) a risk assessment that summarizes the level of inherent risk to the state member bank by risk category and (2) an assessment of the adequacy of board of directors' and management oversight of the insurance and annuity sales activities, including their internal control framework. For those state member banks selling insurance or annuity products, or that enter into arrangements under which another party sells insurance or annuity products at the bank's offices or on behalf of the bank, a second objective of the review is to determine the bank's compliance with the consumer protection provisions of the GLB Act and the CPSI regulation.

State Regulation of Insurance Activities

Historically, insurance activities have primarily been regulated by the states. In 1945, Congress passed the McCarran-Ferguson Act, which granted states the power to regulate most aspects of the insurance business. The McCarran-Ferguson Act states that "no act of Congress shall be construed to invalidate, impair, or supersede any law enacted by any state for the purpose of regulating the business of insurance, or which imposes a fee or tax upon such business, unless such Act specifically relates to the business of insurance" (15 USC 1012(b)).

State regulation of insurance producers is centered on the protection of the consumer and consists primarily of licensing and continuing education requirements for producers. A producer generally must obtain a license from each state in which it sells insurance and for each product sold. Each state in which a producer sells insurance has regulatory authority over the producer's activities in the state.

The GLB Act does include several provisions that are designed to keep states from (1) unfairly regulating a bank to prevent it from engaging in authorized insurance activities or (2) otherwise discriminating against banks engaged in insurance activities. These provisions are complex and beyond the scope of this guidance. However, the GLB Act generally does not prohibit a

4. See section 1001.1 for a discussion of the Federal Reserve's risk-focused examinations and the risk-focused supervision program for community banking organizations.

state from requiring a bank or bank employee engaged in insurance sales, solicitation, or cross-marketing activities to be licensed within the state.

State insurance regulatory authorities do not conduct routine, periodic examinations of an insurance producer. A state examination of an insurance producer is generally conducted only on an ad hoc basis and is primarily based on the volume and severity of consumer complaints. The state examination may also be based in part on the producer's market share and on previous examination findings. Additionally, a review of a producer would typically not assess its financial condition.

A state's market conduct examination of *insurance sales practices* is focused at the insurance-underwriter level.[5] The insurance underwriter is generally held accountable for compliance with state insurance laws to protect the consumer from the unfair sales practices of any producer that markets the insurance underwriter's products. Market conduct examinations of an insurance underwriter may potentially uncover a concern about a particular producer, such as a bank-affiliated producer.[6] However, in the past, a state insurance regulatory authority has not typically examined a producer unless the producer is owned by the insurance underwriter.

Generally, market conduct examinations include reviews of the insurance underwriters' complaint handling, producer licensing, policyholder service, and marketing and sales practices. Typically, a state authority will direct a corrective action for insurance sales activity at the underwriter. The states generally have specific guidance for their market conduct examinations of life, health, and property/casualty[7] lines of business—guidance that corresponds to regulations related to advertising, misrepresentations, and disclosures for these different business lines. The reports of examination issued by the state insurance departments are usually available to the public.

Because the underwriter, not the producer, is liable to the insured, the failure of an insurance producer generally would not result in financial loss to consumers or state guarantee funds. Consequently, there are no regulatory capital requirements for insurance producers, nor do states require regulatory reporting of financial statement data on insurance producers. While the underwriter is ultimately liable to the insured, in some instances, a producer and its owner may be held liable for misrepresentations, as well as for violations of laws and regulations.

Functional Regulation

Under the GLB Act, banking supervisors' reviews of insurance or securities activities conducted in a bank's functionally regulated subsidiary are not to be extensions of more traditional bank-like supervision. Rather, to the extent possible, bank supervisors are to rely on the functional regulators to appropriately supervise the insurance and securities activities of a functionally regulated subsidiary. A functionally regulated subsidiary includes any subsidiary of a bank that (1) is engaged in insurance activities and subject to supervision by a state insurance regulator or (2) is registered as a broker-dealer with the Securities and Exchange Commission. The GLB Act does *not* limit the Federal Reserve's supervisory authority with respect to a *bank* or the insurance activities conducted by a bank. The functional regulators for insurance sales activities, including the activities of insurance producers, consist of the insurance departments in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, American Samoa, and Guam.

The GLB Act places certain limits on the ability of the Federal Reserve to examine, obtain reports from, or take enforcement action against a functionally regulated nondepository subsidiary of a state member bank. For purposes of these limitations, a subsidiary licensed by a state insurance department to conduct insurance sales

5. Generally, market conduct reviews of *insurance underwriters* are conducted on an ad hoc basis, triggered primarily by the volume and severity of consumer complaints, and are based on the underwriter's market share or on previous examination findings. In some states, however, market conduct reviews of insurance underwriters are conducted on a periodic, three- to five-year schedule.

6. The terms "insurance underwriter," "insurer," "insurance carrier,"' and "insurance company" are industry terms that apply similarly to the party to an insurance arrangement who undertakes to indemnify for losses, that is, the party that assumes the principal risk under the contract.

7. Property insurance indemnifies a person who has an interest in a physical property for loss of the property or the loss of its income-producing abilities. Casualty insurance is primarily concerned with the legal liability for losses caused by injury to persons or damage to the property of others. It may also include such diverse forms of insurance as crime insurance, boiler and machinery insurance, and aviation insurance. Many casualty insurers also underwrite surety bonds.

activities is considered functionally regulated only with respect to its insurance activities and any activities incidental to these activities.[8]

The GLB Act indicates that the Federal Reserve must rely, to the fullest extent possible, on information obtained by the appropriate state insurance authority of a nondepository insurance agency subsidiary of a state member bank. In addition, the Federal Reserve may examine a functionally regulated subsidiary of a state member bank only in the following situations:

- The Federal Reserve has reasonable cause to believe that the subsidiary is engaged in activities that pose a material risk to an affiliated depository institution, as determined by the responsible Reserve Bank and Board staff.
- After reviewing relevant information (including information obtained from the appropriate functional regulator), it is determined that an examination is necessary to adequately understand and assess the banking organization's systems for monitoring and controlling the financial and operational risks that may pose a threat to the safety and soundness of an affiliated depository institution.
- On the basis of reports and other available information (including information obtained from the appropriate functional regulator), there is reasonable cause to believe that the subsidiary is not in compliance with a federal law that the Federal Reserve has specific jurisdiction to enforce with respect to the subsidiary (including limits relating to transactions with affiliated depository institutions), and the Federal Reserve cannot assess such compliance by examining the state member bank or other affiliated depository institution.

Other similar restrictions limit the ability of the Federal Reserve to obtain a report directly from, or take enforcement action against, a functionally regulated nonbank subsidiary of a state member bank. These GLB Act limitations do *not* apply to a state member bank even if the state member bank is itself licensed by a state insurance regulatory authority to conduct insurance sales activities. The Board's Division of Consumer and Community Affairs CP Letter 2001 11 outlines the procedures for sharing consumer compliant information with state insurance regulators.

Staff who are conducting reviews of state member bank insurance or annuity sales activities should be thoroughly familiar with SR-00-13, which provides guidance on reviews of functionally regulated state member bank subsidiaries. Reserve Bank staff may conduct an examination of a functionally regulated subsidiary, or request a specialized report from a functionally regulated subsidiary, only after obtaining approvals from the appropriate staff of the Board's Division of Banking Supervision and Regulation.

When preparing or updating the risk assessment of a state member bank's insurance or annuity sales activities, Federal Reserve staff, when appropriate, should coordinate their activities with the appropriate state insurance authorities. The Federal Reserve's supervision of state member banks engaged in insurance sales activities is not intended to replace or duplicate the regulation of insurance activities by the appropriate state insurance authorities.

Information Sharing with the Functional Regulator

The Federal Reserve and the National Association of Insurance Commissioners (NAIC) approved a model memorandum of understanding (MOU) on the sharing of confidential information between the Federal Reserve and individual state insurance departments.[9] The Board also approved the delegation of authority to the Board's general counsel to execute agreements with individual states, based on this MOU. Examiners should follow required Board administrative procedures before sharing any confidential information with a state insurance regulator. (These procedures generally require Federal Reserve staff to identify and forward to Board staff for review any confidential information that may be appropriate to share with the applicable state insurance regulator concerning insurance sales activities conducted by state member banks.)

8. For example, if a state member bank subsidiary engages in mortgage lending and is also licensed as an insurance agency, it would be considered a functionally regulated subsidiary only to the extent of its insurance sales activities.

9. The NAIC is the organization of insurance regulators from the 50 states, the District of Columbia, and the four U. S. territories. The NAIC provides a forum for the development of uniform policy among the states and territories. The NAIC is not a governmental or regulatory body.

STATUTORY AND REGULATORY REQUIREMENTS AND POLICY GUIDANCE

Privacy Rule and the Fair Credit Reporting Act

State member banks that sell insurance to consumers must comply with the privacy provisions under title V of the GLB Act (12 USC 6801–6809), as implemented by the Board's Regulation P (12 CFR 216) (the privacy rule). Functionally regulated state member bank nonbank insurance agency subsidiaries are not covered by the Federal Reserve's privacy rule; however, they must comply with the privacy regulations (if any) issued by their relevant state insurance regulator.

The privacy rule regulates a state member bank's treatment of nonpublic personal information about a ''consumer,'' an individual who obtains a financial product or service (such as insurance) from the institution for personal, family, or household purposes. The privacy rule generally requires a bank to provide a notice to each of its customers that describes its privacy policies and practices no later than when the bank establishes a business relationship with the customer. The privacy rule also generally prohibits a bank from disclosing any nonpublic personal information about a consumer to any nonaffiliated third party, unless the bank first provides to the consumer a privacy notice and a reasonable opportunity to prevent (or ''opt out'' of) the disclosure, and the consumer does not opt out. The privacy rule permits a financial institution to provide a joint notice with one or more of its affiliates or other financial institutions, as identified in the privacy notice itself, provided that the notice is accurate with respect to the institution and the other institutions.

While the privacy rule applies to the sharing of nonpublic personal information by a bank with nonaffiliated third parties, the sharing of certain consumer information with affiliates or nonaffiliates may be subject to the Fair Credit Reporting Act (FCRA) as well. For example, under the FCRA, if a bank wants to share with its insurance subsidiary information from a credit report or from a consumer application for credit (such as the consumer's assets, income, or marital status), the bank must first notify the consumer about the intended sharing and give the consumer an opportunity to opt out. The same rules would apply to an insurance company that wants to share information from credit reports or from applications for insurance with an affiliate or a third party.

Anti-Tying Prohibitions

Federal law (section 106(b) of the BHC Act Amendments of 1970 (12 USC 1972(b))) generally prohibits a bank from requiring that a customer purchase a product or service from the bank or an affiliate as a prerequisite to obtaining another product or service (or a discount on the other product or service) from the bank. This prohibition applies whether the customer is retail or institutional, or whether the transaction is on bank premises or off premises. For example, a state member bank may not require that a customer purchase insurance from the bank or a subsidiary or affiliate of the bank in order to obtain a loan from the bank (or a reduced interest rate on the loan).[10]

Policy Statement on Income from Sale of Credit Life Insurance

The Federal Reserve Board's Policy Statement on Income from Sale of Credit Life Insurance (see the *Federal Reserve Regulatory Service* at 3-1556) sets forth the principles and standards that apply to a bank's sales of credit life insurance and the limitations that apply to the receipt of income from those sales by certain individuals and entities associated with the bank. See also the examination procedures related to this policy statement in section 2130.3.

RISK-MANAGEMENT PROGRAM

Elements of a Sound Insurance or Annuity Sales Program

A state member bank engaged in insurance or annuity sales activities should—

10. See this manual's section 6080.1 "Regulation Y: Prohibitions Against Tying Arrangement" section 3500.0, of the *Bank Holding Company Supervision Manual.*

- conduct insurance sales programs in a safe and sound manner;
- have appropriate written policies and procedures in place that are commensurate with the volume and complexity of its insurance sales activities;
- obtain its board of directors' approval of the scope of the insurance and annuity sales program and of written policies and procedures for the program;
- effectively oversee the sales program activities, including third-party arrangements;
- have an effective, independent internal audit and compliance program;
- appropriately train and supervise the employees conducting insurance and annuity sales activities;
- take reasonable precautions to ensure that disclosures to customers for insurance and annuity sales and solicitations are complete and accurate and are in compliance with applicable laws and regulations;
- ensure compliance with all applicable federal, state, or other jurisdiction regulations, including compliance with sections 23A and 23B of the Federal Reserve Act as that act applies to affiliate transactions; and
- have controls in place to ensure accurate and timely financial reporting.

Every state member bank conducting insurance or annuity sales activities should have appropriate, board-approved policies, procedures, and controls in place to monitor and ensure that it complies with both federal and state regulatory requirements. Consistent with the principle of functional regulation, the Federal Reserve will rely primarily on the appropriate state insurance authorities to monitor and enforce compliance with applicable state insurance laws and regulations, including state consumer protection laws and regulations governing insurance sales.

Sales Practices and Handling of Customer Complaints

Every state member bank engaged in insurance or annuity sales activities should have board-approved policies and procedures for handling customer complaints related to these sales. The customer complaint process should provide for the recording and tracking of all complaints and require periodic reviews of complaints by compliance personnel. A state member bank's board of directors and senior management should also review complaints if the complaints involve significant compliance issues that may pose a risk to the state member bank.

Third-Party Arrangements

State member banks, to the extent permitted by applicable law, may enter into agreements with third parties, including unaffiliated agents or agencies, to sell insurance or annuities or provide expertise and services that otherwise would have to be developed in-house. Many banks hire third parties to assist in establishing an insurance program or to train their own insurance staff. A bank may also find it advantageous to offer more specialized insurance products through a third-party arrangement.

A state member bank's management should conduct a comprehensive review of an unaffiliated third party before entering into any arrangement to conduct insurance or annuity sales with the third party. The review should include an assessment of the third party's financial condition, management experience, and ability to fulfill its contractual obligations to the state member bank, which includes compliance with applicable consumer protection laws and regulations.

The state member bank's board of directors or its designated committee should approve any agreements with third parties. Agreements should outline the duties and responsibilities of each party; describe the third-party activities permitted on the institution's premises; address the sharing or use of confidential customer information; and define the terms for use of the state member bank's office space, equipment, and personnel. If an arrangement includes dual employees (for example, bank employees who are also employed by an independent third party), the agreement must provide for written employment contracts that specify the duties of these employees and their compensation arrangements.

In addition, a third-party agreement should specify that the third party will comply with all applicable laws and regulations and will conduct its activities in a manner consistent with the CPSI regulation, if applicable. The agreement should authorize the banking organization to monitor the third party's compliance with its agreement, as well as authorize the bank to have access to third-party records considered neces-

sary to evaluate compliance. A state member bank that contracts with a functionally regulated third party should obtain from and review, as appropriate, any relevant, publicly available regulatory reports of examination of the third party.[11] Finally, the agreement should provide for indemnification of the institution by the unaffiliated third party for any losses caused by the conduct of the third party's employees in connection with its sales activities.

The state member bank is responsible for ensuring that any third party or dual employee selling insurance at or on behalf of the bank is appropriately trained either by the bank or the third party with respect to compliance with the minimum disclosures and other requirements of the CPSI regulation and applicable state regulations. The banking organization should obtain and review copies of third-party training and compliance materials to monitor the third party's performance of its disclosure and training obligations.

Designation, Training, and Supervision of Personnel

A state member bank hiring personnel to sell insurance or annuities should investigate the backgrounds of the prospective employees. When a candidate for employment has previous insurance industry experience, the state member bank should have procedures to determine whether the individual has been the subject of any disciplinary actions by state insurance regulators.[12]

The state member bank should require its own insurance or annuity sales personnel or third-party sales personnel selling at or on behalf of the bank to receive appropriate training and licensing. Training should cover appropriate policies and procedures for the bank's sales of insurance and annuity products. Personnel who are referring potential or established customers to a licensed insurance producer should also be trained to ensure that referrals are made in conformance with the CPSI regulation, if applicable. The training should also include procedures and guidance to ensure that an unlicensed or referring individual cannot be deemed to be acting as an insurance agent that is subject to licensing requirements.

When insurance or annuities are sold by a state member bank or third parties at an office of, or on behalf of, the organization, the institution should have policies and procedures to designate, by title or name, the individuals responsible for supervising insurance sales activities, as well as for supervising the referral activities of bank employees not authorized to sell these products. A state member bank also should designate supervisory personnel responsible for monitoring compliance with any third-party agreement, as well as with the CPSI regulation, if applicable.

Compliance

State member banks should have policies and procedures to ensure that insurance or annuity sales activities are conducted in compliance with applicable laws and regulations (including the CPSI regulation for sales conducted by or on behalf of the state member bank) and the institution's internal policies and procedures. Compliance procedures should identify any potential conflicts of interest and how such conflicts should be addressed. For example, sales-compensation programs should be conducted in a manner that would not expose the bank to undue legal risks. The compliance procedures should also provide for a system to monitor customer complaints and their resolution. Where applicable, compliance procedures also should call for verification that third-party sales are being conducted in a manner consistent with the governing agreement with the banking organization.

The compliance function should be conducted independently of the insurance and annuity product sales and management activities. Compliance personnel should determine the scope and frequency of their reviews, and findings of compliance reviews should be reported directly to the state member bank's board of directors or to its designated board committee.

11. The reports of examination issued by state insurance regulators are generally public documents. Many states do not conduct periodic examinations of insurance sales activities.

12. Information from the states on the issuance and termination of producer licenses and on producers' compliance with continuing education requirements is available from the NAIC database known as the National Insurance Producer Registry (NIPR).

RISK ASSESSMENT OF INSURANCE AND ANNUITY SALES ACTIVITIES

A risk assessment of insurance activities may be accomplished in the course of conducting a regularly scheduled state member bank examination or as a targeted review. The purpose of preparing the risk assessment is to determine the level and direction of risk to the bank arising from its insurance and annuity sales activities. Risks to state member banks engaged in insurance and annuity sales programs consist primarily of legal and operational risk, all of which may lead to financial loss. After completing the risk assessment, if material concerns remain, the Board's Division of Banking Supervision and Regulation staff should be consulted for further guidance.

Legal risk may arise from a variety of sources, such as fraud; noncompliance with statutory or regulatory requirements, including those pertaining to the handling of premiums collected on behalf of the underwriter; claims processing; insurance and annuity sales practices; and the handling of "errors and omissions" claims.[13] Other sources of legal risk may arise from failing to safeguard nonpublic customer information, a high volume of customer complaints, or public regulatory sanctions against a producer.

Legal risks may also arise from an agent's obligation to provide a customer with products that are suited to the customer's particular needs and are priced and sold in accordance with state regulations. Additionally, an agent or agency may be liable for failing to carry out the appropriate paperwork to bind a policy that it has sold to a customer, or for making an error in binding the policy. State insurance departments generally are permitted by law to suspend or revoke a producer's license and assess monetary penalties against a producer if warranted.

Operational risk may arise from errors in processing sales-related information or from a lack of appropriate controls over systems or staff responsible for carrying out the insurance or annuity sales activities. Additionally, state member banks that have recently commenced insurance or annuity sales activities, or that are expanding their insurance or annuity sales business, also are exposed to risk arising from inadequate strategic and financial planning associated with the activities, which could result in financial loss. Examiners should be attuned to risks that may arise from inadequate controls over insurance activities, a rapid expansion of the insurance or annuity sales programs offered by the state member bank, the introduction of new products or delivery channels, and legal and regulatory developments.

Operational risk may arise from inadequate premium-payment procedures and trust-account-balance administration by an agency. When the insurance agency bills the insured, the agent must comply with requirements for forwarding the payments to the insurer and for safekeeping the funds. Inadequate internal controls over this activity may result in the inappropriate use of these funds by the agent or agency. The state member bank should ensure that appropriate controls are in place to verify that all funds that are owed to the insurer or the insured are identified in the trust account and that the account is in balance.

When conducting a risk assessment, the examiner should first obtain relevant information to determine the existence and scale of insurance or annuity sales activity. Such information is available in the state member bank's Uniform Bank Performance Report (UBPR) and in other System reports on insurance activities. Relevant reports, including applicable balance sheets and income statements for the insurance and annuity sales activities, may also be obtained from the state member bank. When preparing a risk assessment for an insurance or annuity sales activity that is conducted by a functionally regulated nonbank subsidiary of a state member bank, examiners should rely, to the fullest extent possible, on information available from the state member bank and the appropriate state insurance regulator for the subsidiary. If information that is needed to assess the risk cannot be obtained from the state member bank or the applicable functional regulator, the examiner should consult with the appropriate designated Board staff. Requests should not be made directly to a functionally regulated nonbank insurance and annuity sales subsidiary of a state member bank without first obtaining approval from the appropriate Board staff.

13. Errors and omissions insurance indemnifies the insured against loss sustained because of an error or oversight by the insured. For instance, an insurance agency generally purchases this type of coverage to protect itself against such things as failing to issue a policy.

CONSUMER PROTECTION IN SALES OF INSURANCE RULES

Overview of the CPSI Regulation

The CPSI regulation is applicable to all insured depository institutions.[14] The regulation, however, generally does not apply to nonbank affiliates or subsidiaries of a state member bank unless the company engages in the retail sale of insurance products or annuities at an office of, or on behalf of, an insured depository institution. Interpretations of the regulation issued by the federal banking agencies are found in appendix A of this section. Federal Reserve examiners are responsible for reviewing state member banks' compliance with the regulation.

The regulation applies to the retail sale of insurance products and annuities by banks or by any other person at an office of a bank, or acting on behalf of a bank. For purposes of the CPSI regulation, "office" means the premises of the bank where retail deposits are accepted. The regulation applies only to the retail sale of insurance or annuity products—that is, when the insurance is sold or marketed to an individual primarily for personal, family, or household purposes.

Misrepresentations Prohibited

The regulation prohibits a bank or other covered person from engaging in any practice or using any advertisement at any office of, or on behalf of, the bank or a subsidiary of the bank if the practice or advertisement could mislead any person or otherwise cause a reasonable person to erroneously believe—

- that the insurance product or annuity is backed by the federal government or the bank or is insured by the Federal Deposit Insurance Corporation (FDIC);
- that an insurance product or annuity does not have investment risk, including the potential that principal may be lost and the product may decline in value, when in fact the product or annuity does have such risks; or
- in the case of a bank or subsidiary of the bank at which insurance products or annuities are sold or offered for sale, that (1) the bank may condition approval of an extension of credit to a consumer by the bank or subsidiary on the purchase of an insurance product or annuity from the bank or a subsidiary of the bank, and (2) the consumer is not free to purchase the insurance product or annuity from another source.

The regulation also incorporates the anti-tying provisions of section 106(b) of the Bank Holding Company Act Amendments of 1970 (12 USC 1972). Additionally, banks are prohibited from selling life or health insurance products if the status of the applicant or insured as a victim of domestic violence or as a provider of services to domestic violence victims is considered as a factor in decision making on the product, except as expressly authorized by state law.

Insurance Disclosures

The CPSI regulation also requires that a bank or a person selling insurance at an office of, or on behalf of, a bank make the following affirmative disclosures (to the extent accurate), both orally and in writing, before the completion of the initial sale of an insurance product or an annuity to a consumer. However, sales by mail or, if the consumer consents, via electronic media (such as the Internet) do not require oral disclosure.

- The insurance product or annuity is not a deposit or other obligation of, or guaranteed by, the bank or an affiliate of the bank.
- The insurance product or annuity is not insured by the FDIC or any other U.S. government agency, the bank, or (if applicable) an affiliate of the bank.
- The insurance product or annuity, if applicable, has investment risk, including the possible loss of value.

For telephone sales, written disclosures must be mailed within three business days. The above disclosures must be included in advertisements and promotional materials for insurance products and annuities, unless the advertisements or promotional materials are of a general nature and describe or list the nature of services or products offered by the bank. Disclosures must be conspicuous and readily understandable.

14. The CPSI regulation applies to all federally insured depository institutions, including all federally chartered U.S. branches and state-chartered insured U.S. branches of foreign banking organizations.

Credit Disclosures

When an application for credit is made in connection with the solicitation, offer, or sale of an insurance product or annuity, the consumer must be notified that the bank may not condition the extension of credit on either (1) the consumer's purchase of an insurance product or annuity from the bank or any of its affiliates or (2) the consumer's agreement not to obtain, or a prohibition on the consumer from obtaining, an insurance product or annuity from an unaffiliated entity. These disclosures must be made both orally and in writing; however, applications taken by mail or, if the consumer consents, via electronic media, do not require oral disclosure. For telephone applications, the written disclosure must be mailed within three business days. The disclosures must be conspicuous and readily understandable.

Consumer Acknowledgment

The bank must obtain written or electronic acknowledgments of the consumer's receipt of the disclosures described above at the time they are made or at the completion of the initial purchase. For telephone sales, the bank must receive an oral acknowledgment and make a reasonable effort to obtain a subsequent written or electronic acknowledgment.

Location

Insurance and annuity sales activities must take place, to the extent practicable, in an area physically segregated from one where retail deposits are routinely accepted from the general public (such as teller windows). The bank must clearly identify and delineate areas where insurance and annuity sales activities occur.

Referrals

Any person who accepts deposits from the public in an area where deposits are routinely accepted may refer a consumer to a qualified person who sells insurance products or annuities only if the person making the referral receives no more than a one-time, nominal fee of a fixed dollar amount for the referral. The amount of the referral fee may *not* depend on whether a sale results from the referral.

Qualifications

A bank may not permit any person to sell or offer insurance products or annuities at its office or on its behalf, unless that person is at all times properly qualified and licensed under applicable state law for the specific products being sold or recommended.

Relationship of the CPSI Regulation to State Regulation

The GLB Act contains a legal framework for determining the effect of the CPSI regulation on state laws governing the sale of insurance, including state consumer protection standards. In general, if a state has legal requirements that are inconsistent with, or contrary to, the CPSI regulation, initially the federal regulation does not apply in the state. However, the federal banking agencies may, after consulting with the state involved, decide to preempt any inconsistent or contrary state laws if the agencies find that the CPSI regulation provides greater protections than the state laws. It is not expected that there will be significant conflict between state and federal laws in this area. If the consumer protection laws of a particular state appear to be inconsistent with and less stringent (that is, provide less consumer protection) than the CPSI regulation, examiners should inform the staff of the Board's Division of Banking Supervision and Regulation.

Relationship to Federal Reserve Guidance on the Sale of Nondeposit Investment Products

When a bank sells insurance products or annuities that also are securities (such as variable life insurance annuities), it must conform with the applicable Federal Reserve and interagency guidance pertaining to a bank's retail sales of nondeposit investment products (NDIPs).[15] If the

15. Interagency Statement on Retail Sales of Nondeposit Investment Products, February 17, 1994. See SR-94-11.

CPSI regulation and the guidance pertaining to NDIPs conflict, the CPSI regulation prevails.

Examining a State Member Bank for Compliance with the CPSI Regulation

Examinations for compliance with the CPSI regulation should be conducted consistent with the risk-focused supervisory approach when a state member bank sells insurance products or annuities directly, or when a third party sells insurance or annuities at or on behalf of, a state member bank. To the extent practicable, the examiner should conduct the review at the state member bank. In certain instances, however, the examiner's review at the state member bank may identify potential supervisory concerns about the state member bank's compliance with the CPSI regulation as it pertains to insurance or annuities sales conducted by a functionally regulated nonbank affiliate or subsidiary of the state member bank that is selling insurance products or annuities at or on behalf of the state member bank.

If the examiner determines that an on-site review of a functionally regulated nonbank affiliate or subsidiary of the state member bank is appropriate to adequately assess the state member bank's compliance with the CPSI regulation, the examiner should discuss the situation with staff of the Board's Division of Banking Supervision and Regulation. The approval of the Division of Banking Supervision and Regulation's officer that is responsible for the supervisory policy and examination guidance pertaining to insurance and annuity sales activities should be obtained before examining or requesting any information directly from a functionally regulated nonbank affiliate or subsidiary of the state member bank that is selling insurance or annuity products at or on behalf of the state member bank.

The examination guidelines described in section 4043.3 apply to retail sales, solicitations, advertisements, or offers of insurance products and annuities by any state member bank or any other person that is engaged in such activities at an office of the bank or on behalf of the state member bank. For purposes of the CPSI regulation, activities ''on behalf of a state member bank'' include activities in which a person, whether at an office of the bank or at another location, sells, solicits, advertises, or offers an insurance product or annuity and in which at least one of the following applies:

- The person represents to a consumer that the sale, solicitation, advertisement, or offer of any insurance product or annuity is by or on behalf of the bank.
- The bank refers a consumer to a seller of insurance products or annuities, and the bank has a contractual arrangement to receive commissions or fees derived from the sale of an insurance product or annuity resulting from the bank's referral.
- Documents evidencing the sale, solicitation, advertising, or offer of an insurance product or annuity identify or refer to the bank.

APPENDIX A—JOINT INTERPRETATIONS OF THE CONSUMER PROTECTION IN SALES OF INSURANCE REGULATION

In response to a banking association's inquiries, the federal banking agencies jointly issued interpretations regarding the Consumer Protection in Sales of Insurance (CPSI) regulation.[1] A joint statement, issued on August 17, 2001, contains responses to a set of questions relating to disclosure and acknowledgment, the scope of applicability of the regulation, and compliance. Additionally, a February 28, 2003, joint statement responded to a request to clarify whether the disclosure requirements apply to renewals of pre-existing insurance policies sold before October 1, 2001, the effective date of the regulation. The issues raised and the banking agencies' responses are summarized below.

Disclosures

Credit Disclosures

A bank or other person who engages in insurance sales activities at an office of, or on behalf of, a bank (''a covered person'') must make the

1. These letters, issued jointly by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision, may be accessed on these agencies' web sites.

credit disclosures set forth in the regulation if a consumer is solicited to purchase insurance while the consumer's loan application is pending. A consumer's application for credit is still "pending" for purposes of the regulation if the depository institution has approved the consumer's loan application but not yet notified the consumer. Until the consumer is notified of the loan approval, the covered person must provide the credit disclosures if the consumer is solicited, offered, or sold insurance.

Disclosures for Sales by Mail and Telephone

The regulation requires a covered person to provide oral disclosures and to obtain an oral acknowledgment of these disclosures when sales activities are conducted by telephone. This requirement applies regardless of whether the consumer will also receive and acknowledge written disclosures in person, through the mail, or electronically.

Use of Short-Form Insurance Disclosures

There is no short form for the credit disclosures. A depository institution, however, may use the short-form insurance disclosures set forth below in visual media (such as television broadcasting, ATM screens, billboards, signs, posters, and written advertisements and promotional materials):

- NOT A DEPOSIT
- NOT FDIC-INSURED
- NOT INSURED BY ANY FEDERAL GOVERNMENT AGENCY
- NOT GUARANTEED BY THE BANK
- MAY GO DOWN IN VALUE

Acknowledgment of Disclosures

Reasonable efforts to obtain written acknowledgment. The banking agencies have not prescribed any steps that must be taken for a depository institution's efforts to obtain a written acknowledgment to be deemed "reasonable" in a transaction conducted by telephone. Examples of reasonable efforts, however, include—

- providing the consumer with a return-addressed envelope or similar means to facilitate the consumer's return of the written acknowledgment,
- making a follow-up phone call or contact,
- sending a second mailing, or
- similar actions.

The covered person should (1) maintain documentation that the written disclosures and the request for written acknowledgment of those disclosures were mailed to the consumer and (2) should record his or her efforts to obtain the signed acknowledgment. The "reasonable efforts" policy exception for telephone sales does not apply to other types of transactions, such as mail solicitations, in which a covered person must obtain from the consumer a written (in electronic or paper form) acknowledgment.

Appropriate form or format for acknowledgment provided electronically. Electronic acknowledgments are not required to be in a specific format but must be consistent with the provisions of the CPSI regulation applicable to consumer acknowledgments. That is, the electronic acknowledgment must establish that the consumer has acknowledged receipt of the credit and insurance disclosures, as applicable.

Retention of acknowledgments by an insurance company. If an insurance company provides the disclosures and obtains the acknowledgment on behalf of a depository institution, the insurance company may retain the acknowledgment. The depository institution is responsible for ensuring that sales made "on behalf of" the depository institution are in compliance with the CPSI regulation. An insurance company may maintain documentation showing compliance with the CPSI regulation, but the depository institution should have access to such records and the records should be readily available for review by examiners.

Form of written acknowledgment. There is no prescribed form for the written acknowledgment. The regulation requires, however, that a covered person obtain the consumer's acknowledgment of receipt of the complete insurance and credit disclosures.

Timing of acknowledgment receipt. A covered person must obtain the consumer's acknowledgment either at the time a consumer receives

disclosures or at the time of the initial purchase of an insurance product.

Oral acknowledgment of oral disclosure. The CPSI regulation does not prescribe any specific wording for an oral acknowledgment. However, if a covered person has made the insurance and credit disclosures orally, an affirmative response to the question "Do you acknowledge that you received this disclosure?" is acceptable.

Scope of the CPSI Regulation

Applicability to Private Mortgage Insurance

Depending on the nature of a depository institution's involvement in an insurance sales transaction, the CPSI regulation may cover sales of private mortgage insurance. If the depository institution itself purchases the insurance to protect its interest in mortgage loans it has issued and merely passes the costs of the insurance on to the mortgage borrowers, the transaction is not covered by the regulation. If, however, a consumer has the option of purchasing the private mortgage insurance and (1) the depository institution offers the private mortgage insurance to a consumer or (2) any other person offers the private mortgage insurance to a consumer at an office of a depository institution, or on behalf of a depository institution, the transaction would be covered by the regulation.

Applicability to Federal Crop Insurance

The CPSI regulation does not apply to federal crop insurance that is sold for commercial or business purposes. However, if the crop insurance is purchased by an individual primarily for family, personal, or household purposes, it would be covered.

Solicitations and Applications Distributed Before, but Returned After, the Effective Date of the CPSI Regulation

Direct-mail solicitations and "take-one" applications that are distributed on or after October 1, 2001, must comply with the CPSI regulation. If a consumer seeks to purchase insurance after the effective date of the regulation in response to a solicitation or advertisement that was distributed *before* that date, the depository institution would be in compliance with the regulation if the institution provides the consumer, before the initial sale, with the disclosures required by the regulation. These disclosures must be both written and oral, except that oral disclosures are not required if the consumer mails in the application.

Renewals of Insurance

Renewals of insurance are not subject to the disclosure requirements (see "Disclosures" above) but are subject to other requirements of the CPSI regulation. A "renewal" of insurance means continuation of coverage involving the same type of insurance for a consumer as issued by the same carrier. A renewal need not be on the same terms and conditions as the original policy, provided that the renewal does not involve a different type of insurance and the consumer has previously received the disclosures required by the regulation at the time of the initial sale. An upgrade in coverage at a time when a policy is not up for renewal would be treated as a renewal, provided that the solicitation and sale of the upgrade does not involve a different type of insurance and the consumer has previously received the disclosures required by the regulation at the initial sale.

Disclosures Required with Renewals of Insurance Coverage

The banking agencies' interpretations clarified that the CPSI regulation does not *mandate* disclosures for renewals of policies sold before October 1, 2001. Accordingly, the regulation does not require the disclosures to be furnished at the time of renewal of a policy, including a pre-existing policy. However, renewals are subject to the other provisions of the regulation. Moreover, the banking agencies would expect that, consistent with applicable safety-and-soundness requirements, depository institutions would take reasonable steps to avoid customer confusion in connection with renewals of pre-existing policies.

"On-Behalf-of" Test and Use of Corporate Name or Logo

Under the CPSI regulation, an affiliate of a bank is not considered to be acting "on behalf of" a bank simply because the affiliate's marketing or other materials use a corporate name or logo that is common to the bank and the affiliate. In general, this exclusion applies even if a bank and its parent holding company have a similar, but not identical, name. For example, if the names of all of the affiliates of a bank holding company share the words "First National," an affiliate would not be considered to be engaged in an activity "on behalf of" an affiliated bank simply by using the terms "First National" as part of a corporate logo or identity. The affiliate would, however, be considered to be acting "on behalf of" an affiliated bank if the name of the bank (for example, "First National Bank") appears in a document as the seller, solicitor, advertiser, or offeror of insurance. A transaction also would be covered if it occurs on the premises of a depository institution or if one of the other prongs of the "on-behalf-of" test is met.

Compliance

Appropriate Documentation of an Oral Disclosure or Oral Acknowledgment

There is no specific documentation requirement for oral disclosures or acknowledgments. However, other applicable regulatory reporting standards would apply. Appropriate documentation of an oral disclosure would clearly show that the covered person made the credit and insurance disclosures to a consumer. Similarly, appropriate documentation of an oral acknowledgment would clearly show that the consumer acknowledged receiving the credit and insurance disclosures. For example, a tape recording of the conversation (where permitted by applicable laws) in which the covered person made the oral disclosures and received the oral acknowledgment would be acceptable. Another example would be a contemporaneous checklist completed by the covered person to indicate that he or she made the oral disclosures and received the oral acknowledgment. A contemporaneous note to the consumer's file would also be adequate. The documentation should be maintained in the consumer's file so that it is accessible to examiners.

Setting for Insurance Sales

A depository institution must identify the areas where insurance sales occur and must clearly delineate and distinguish those areas from areas where the depository institution's retail deposit-taking activities occur. Although the banking agencies did not define how depository institutions could "clearly delineate and distinguish" insurance areas, signage or other means may be used.

APPENDIX B—GLOSSARY

For additional definitions of insurance terms, see section 4040.1.

Accident and health insurance. A type of coverage that pays benefits in case of sickness, accidental injury, or accidental death. This coverage may provide for loss of income when the insured is disabled and provides reimbursement for medical expenses when the insured is ill. The insurance can provide for debt payment if it is taken out in conjunction with a loan. (See *Credit life insurance.*)

Actuary. A professional whose function is to calculate statistically various estimates for the field of insurance, including the estimated risk of loss on an insurable interest and the appropriate level for premiums and reserves.

Admitted insurer. An insurance company licensed by a state insurance department to underwrite insurance products in that state.

Agency contract (or agreement). An agreement that establishes the contractual relationship between an agent and an insurer.

Agent. A licensed insurance company representative under contract to one or more insurance companies. Depending on the line of insurance represented, an agent's power may include soliciting, advertising, and selling insurance; collecting premiums; claims processing; and effecting insurance coverage on behalf of an insurance underwriter. Agents are generally com-

pensated by commissions on policies sold, although some may receive salaries.

- *Captive or exclusive agent.* An agent who represents a single insurer.

- *General agent.* An agent who is contractually awarded a specific geographic territory for an individual insurance company. They are responsible for building their own agency and usually represent only one insurer. Unlike exclusive agents, who usually receive a salary in addition to commissions, general agents are typically compensated on a commission basis only.

- *Independent agent.* An agent who is under contractual agreements with at least two different insurers. Typically, all of the independent agent's compensation originates from commissions.

Aggregate excess-of-loss reinsurance. A form of "excess-of-loss" reinsurance that indemnifies the ceding company against the amount by which all of the ceding company's losses incurred during a specific period (usually 12 months) exceed either (1) a predetermined dollar amount or (2) a percentage of the company's subject premiums. This type of contract is also commonly referred to as *stop-loss reinsurance* or *excess-of-loss ratio reinsurance.*

Allied lines. Various insurance coverages for additional types of losses and against losses by additional perils. The coverages are closely associated with and usually sold with fire insurance. Examples include coverage against loss by perils other than fire, coverage for sprinkler-leakage damage, and business-interruption coverage.

Annuity. A contract that provides for a series of payments payable over an individual's life span or other term, on the basis of an initial lump-sum contribution or series of payments made by the annuitant into the annuity during the accumulation phase of the contract.

- *Fixed-annuity contracts* provide for payments to annuitants at fixed, guaranteed minimum rates of interests.

- *Variable-annuity contracts* provide for payments based on the performance of annuity investments. Variable-annuity contracts are usually sold based on a series of payments and offer a range of investment or funding options, such as stocks, bonds, and money market fund investments. The annuity principal and the investment return are not guaranteed as they depend on the performance of the underlying funding option.

Annuity payments may commence with the execution of the annuity contract (*immediate annuity*) or may be deferred until some future date (*deferred annuity*).

Assigned risk. A risk that is not usually acceptable to insurers and is therefore assigned to a group of insurers who are required to share in the premium income and losses, in accordance with state requirements, in order for the insurer to sell insurance in the state.

Assignment. The legal transfer of one person's interest in an insurance policy to another person or business.

Bank-owned life insurance (BOLI). Life insurance purchased and owned by a bank to fund its exposure arising from employee compensation and benefit programs. In a typical BOLI program, a bank insures a group of employees; pays the life insurance policy premiums; owns the cash values of the policies, which are booked on the bank's balance sheet as "other assets"; and is the beneficiary of the policies upon the death of any insured employee or former employee. (See SR-04-19 and section 4042.1.)

Beneficiary. The person or entity named in an insurance policy as the recipient of insurance proceeds upon the policyholder's death or when an endorsement matures. A revocable beneficiary can be changed by the policyholder at any time. An irrevocable beneficiary can be changed by the policyholder only with the written permission of the beneficiary.

Binder. A written or oral agreement, typically issued by an insurer, agent, or broker for property and casualty insurance, to indicate acceptance of a person's application for insurance and to provide interim coverage pending the insurance company's issuance of a binding policy.

Blanket bond. Coverage for an employer for loss incurred as a result of employee dishonesty.

Boiler and machinery insurance. Insurance against the sudden and accidental breakdown of boilers, machinery, and electrical equipment, including coverage for damage to the equipment and property damage, including the property of others. Coverage can be extended to cover consequential losses, including loss from interruption of business.

Broker. A person who represents the insurance buyer in the purchase of insurance. Brokers do not have the power to bind an insurance company to an insurance contract. Once a contract is accepted, the broker is compensated for the transaction through a commission from the insurance company. An individual may be licensed as both a broker and an agent.

Bulk reinsurance. A transaction sometimes defined by statute as any quota-share, surplus aid, or portfolio reinsurance agreement through which an insurer assumes all or a substantial portion of the liability of the reinsured company.

Captive insurer. An insurance company established by a parent firm to insure or reinsure its own risks or the risks of affiliated companies. A captive may also underwrite insurable risks of unaffiliated companies, typically the risks of its customers or employees. A captive insurer may underwrite credit life or private mortgage insurance (third-party risks) related to its lending activities.

Cash surrender value of life insurance. The amount of cash available to a life insurance policyholder upon the voluntary termination of a life insurance policy before it becomes payable by death or maturity.

Casualty insurance. Coverage for the liability arising from third-party claims against the insured for negligent acts or omissions causing bodily injury or property damage.

Cede. To transfer to a reinsurer all or part of the insurance or reinsurance risk underwritten by an insurance company.

Ceding commission. The fee paid to a reinsurance company for assuming the risk of a primary insurance company.

Ceding company (also cedant, reinsured, reassured). The insurer that transfers all or part of the insurance or reinsurance risk it has underwritten to another insurer or reinsurer via a reinsurance agreement.

Cession. The amount of insurance risk transferred to the reinsurer by the ceding company.

Churning. The illegal practice wherein a customer is persuaded to unnecessarily cancel one insurance policy in favor of buying a purportedly superior policy, often using the cash surrender value of the existing policy to pay the early premiums of the new policy. In such a transaction, the salesperson benefits from the additional commission awarded for booking a new policy.

Claim. A request for payment of a loss under the terms of a policy. Claims are payable in the manner suited to the insured risk. Life, property, casualty, health, and liability claims generally are paid in a lump sum after the loss is incurred. Disability and loss-of-time claims are paid periodically during the period of disability or through a discounted lump-sum payment.

Coinsurance. A provision in property and casualty insurance that requires the insured to maintain a specified amount of insurance based on the value of the property insured. Coinsurance clauses are also found in health insurance and require the insured to share a percentage of the loss.

Combination-plan reinsurance. A reinsurance agreement that combines the excess-of-loss and the quota-share forms of coverage within one contract, with the reinsurance premium established as a fixed percentage of the ceding company's subject premium. After deducting the excess recovery on any one loss for one risk, the reinsurer indemnifies the ceding company on the basis of a fixed quota-share percentage. If a loss does not exceed the excess-of-loss retention level, only the quota-share coverage applies.

Commission. The remuneration paid by insurance carriers to insurance agents and brokers for the sale of insurance and annuity products.

Comprehensive personal liability insurance. A type of insurance that reimburses the policyholder if he or she becomes liable to pay money for damage or injury he or she has caused to others. This coverage does not include automobile liability but does include almost every activity of the policyholder, except business operations.

Contractholder. The person, entity, or group to whom an annuity is issued.

Credit for reinsurance. A statutory accounting procedure, set forth under state insurance regulations, that permits a ceding company to treat amounts due from reinsurers as assets, or as offsets to liabilities, on the basis of the reinsurer's status.

Credit life insurance. A term insurance product issued on the life of a debtor that is tied to repayment of a specific loan or indebtedness. Proceeds of a credit life insurance policy are used to extinguish remaining indebtedness at the time of the borrower's death. The term is applied broadly to other forms of credit-related insurance that provide for debt satisfaction in the event of a borrower's disability, accident or illness, and unemployment. Credit life insurance has historically been among the most common bank insurance products.

Credit score. A number that is based on an analysis of an individual's credit history and that insurers may consider as an indicator of risk for purposes of underwriting insurance. Where not prohibited by state law, insurers may consider a person's credit history when underwriting personal lines.

Debt-cancellation contract/debt-suspension agreement. A loan term or contract between a lender and borrower whereby, for a fee, the lender agrees to cancel or suspend payment on the borrower's loan in the event of the borrowers's death, serious injury, unemployment, or other specified events. The Office of the Comptroller of the Currency considers these products to be banking products. State law determines whether these products are bank or insurance products for state-chartered banks and insurance companies.

Deductible. The amount a policyholder agrees to pay toward the total amount of insurance loss. The deductible may apply to each claim for a loss occurrence, such as each automobile accident, or to all claims made during a specified period, as with health insurance.

Directors and officers liability insurance. Liability insurance covering a corporation's obligation to reimburse its directors or officers for claims made against them for alleged wrongful acts. It also provides direct coverage for company directors and officers themselves in instances when corporate indemnification is not available.

Direct premiums written. Premiums received by an underwriter for all policies written during a given time period by the insurer, excluding those received through reinsurance assumed.

Direct writer. An insurance company that deals directly with the insured through a salaried representative, as opposed to those insurers that use agents. This term also refers to insurers that operate through exclusive agents. In reinsurance, a direct writer is the company that originally underwrites the insurance policies ceded.

Disability income insurance. An insurance product that provides income payment to the insured when his or her income is interrupted or terminated because of illness or accident.

Endowment insurance. A type of life insurance contract under which the insured receives the face value of the policy if he or she survives the endowment period. Otherwise, the beneficiary receives the face value of the policy upon the death of the insured.

Errors and omissions (E&O) liability insurance. Professional liability insurance that covers negligent acts or omissions resulting in loss. Insurance agents are continually exposed to the claim that inadequate or inappropriate coverage was recommended, resulting in a lack of coverage for losses incurred. The agent or the carrier may be responsible for coverage for legitimate claims.

Excess-of-loss reinsurance. A form of reinsurance whereby an insurer pays the amount of each claim for each risk up to a limit determined in advance, and the reinsurer pays the amount of the claim above that limit up to a specific sum. It includes various types of reinsurance, such as

catastrophe reinsurance, per-risk reinsurance, per-occurrence reinsurance, and aggregate excess-of-loss reinsurance.

Excess-per-risk reinsurance. A form of excess-of-loss reinsurance that, subject to a specified limit, indemnifies the ceding company against the amount of loss in excess of a specified retention for each risk involved in each occurrence.

Excess and surplus lines. Property/casualty coverage that is unavailable from insurers licensed by the state (admitted insurers) and must be purchased from a nonadmitted underwriter.

Exposure. The aggregate of all policyholder limits of liability arising from policies written.

Face amount. The amount stated on the face of the insurance policy to be paid, depending on the type of coverage, upon death or maturity. It does not include dividend additions or additional amounts payable under accidental death or other special provisions.

Facultative reinsurance. Reinsurance of individual risks by offer and acceptance wherein the reinsurer retains the faculty to accept or reject each risk offered by the ceding company.

Facultative treaty. A reinsurance contract under which the ceding company has the option to cede and the reinsurer has the option to accept or decline classified risks of a specific business line. The contract merely reflects how individual facultative reinsurance shall be handled.

Financial guarantee insurance. Financial guarantee insurance is provided for a wide array of financial risks. Typically, coverage is provided for the fulfillment of a specific financial obligation originated in a business transaction. The insurer, in effect, is lending the debtor its own credit rating to enhance the debtor's creditworthiness.

Financial strength rating. Opinion as to an insurance company's ability to meet its senior policyholder obligations and claims. For many years, the principal rating agency for property and casualty insurers and life insurers has been A.M. Best. Other rating agencies, such as Fitch, Moody's, Standard and Poor's, and Weiss, also rate insurers.

Fixed annuity. See *Annuity.*

Flood insurance. A special insurance policy to protect against the risk of loss or damage to property caused by flooding. Regular homeowners' policies do not pay for damages caused by flooding.

General liability insurance. A broad commercial policy that covers all business liability exposures, such as product liability, completed operations, premises and operations, independent contractors, and other exposures that are not specifically excluded.

Gross premiums written. Total premiums for insurance written during a given period, before deduction for reinsurance ceded.

Group insurance. Insurance coverage typically issued to an employer under a master policy for the benefit of employees. The insurer usually does not condition coverage of the people that make up the group upon satisfactory medical examinations or other requirements. The individual members of the group hold certificates as evidence of their insurance.

Health insurance. An insurance product that provides benefits for medical expenses incurred as a result of sickness or accident, as well as income payments to replace lost income when the insured is unable to work because of illness, accident, or disability. This product may be in the form of traditional indemnity insurance or managed-care plans and may be underwritten on an individual or group basis.

Incurred but not reported (IBNR). The loss-reserve value established by insurance and reinsurance companies in recognition of their liability for future payments on losses that have occurred but have not yet been reported to them. This definition is often erroneously expanded to include adverse loss development on reported claims. The term *incurred but not enough reported (IBNER)* is being increasingly used to reflect more accurately the adverse development on inadequately reserved reported claims.

Inland marine insurance. A broad field of insurance that covers cargo being shipped by air, truck, or rail. It includes coverage for most property involved in transporting cargo as well as for bridges, tunnels, and communications systems.

Key person life insurance. Life insurance designed to cover the key employees of an employer. It may be written on a group- or an individual-policy basis.

Lapse. The termination or discontinuance of a policy resulting from the insured's failure to pay the premium due.

Liability insurance. Protects policyholders from financial loss due to liability resulting from injuries to other persons or damage to their property.

Lines. A term used in insurance to denote insurance business lines, as in "commercial lines" and "personal lines."

Long-term care insurance. Health insurance designed to supplement the cost of nursing home care or other care facilities in the event of a long-term illness or permanent disability or incapacity.

Managing general agent. A managing general agent (MGA) is a wholesaler of insurance products and services to insurance agents. An MGA receives contractual authority from an insurer to assume many of the insurance company's functions. The MGA may provide insurance products to the public through local insurance agents as well as provide services to an insurance company, including marketing, accounting, data processing, policy maintenance, and claims-monitoring and -processing services. Many insurance companies prefer the MGA distribution and management system for their insurance products because it avoids the high cost of establishing branch offices. Most states require that an MGA be licensed.

Manuscript policy. A policy written to include specific coverage or conditions not provided in a standard policy.

Morbidity. The incidence and severity of illness and disease in a defined class of insured persons.

Mortality. The rate at which members of a group die in a specified period of time or die from a specific illness.

Mortgage guarantee insurance. A product that insures lenders against nonpayment by borrowers. The policies are issued for a specified time period. Lenders who finance more than 80 percent of the property's fair value generally require such insurance.

Mortgage insurance. Life insurance that pays the balance of a mortgage even if the borrower dies. Coverage typically is in the form of term life insurance, with the coverage declining as the debt is paid off.

Multiperil insurance. An insurance contract providing coverage against many perils, usually combining liability and physical damage coverage.

Net premiums written. The amount of gross premiums written, after deduction for premiums ceded to reinsurers.

Ninety-day loss rule. A state requirement for an insurer to establish a loss provision for reinsurance recoverables over 90 days past due.

Obligatory treaty. A reinsurance contract under which business must be ceded in accordance with contract terms and must be accepted by the reinsurer.

Policyholder. The person or entity who owns an insurance policy. This is usually the insured person, but it may also be a relative of the insured, a partnership, or a corporation.

Premium. The payment, or one of the periodic payments, a policyholder agrees to make for insurance coverage.

Private mortgage insurance (PMI). Coverage for a mortgage lender against losses due to a collateral shortfall on a defaulted residential real estate loan. Most banks require borrowers to take out a PMI policy if a downpayment of less than 20 percent of a home's value is made at the time the loan is originated. PMI does not directly benefit a borrower, although its existence provides the opportunity to purchase a home to many people who otherwise would not qualify for a loan.

Producer. A person licensed to sell, solicit, or negotiate insurance.

Professional designations and organizations. Three of the most common insurance professional designations are chartered life under-

writer (CLU), chartered property casualty underwriter (CPCU), and chartered financial consultant (ChFC). Insurance agents also join professional organizations such as the American Society of Chartered Life Underwriters, the International Association of Financial Planning, the National Association of Life Underwriters, the National Association of Health Underwriters, the American Council of Life Insurance, the Life Insurance Marketing and Research Association, the Life Underwriter Training Council, and the Million Dollar Round Table.

Pro rata reinsurance. A generic term describing all forms of "quota-share" and "surplus reinsurance," in which the reinsurer shares a pro rata portion of the losses and premiums of the ceding company.

Property insurance. Coverage for physical damage or destruction of real property (buildings, fixtures, and permanently attached equipment) and personal property (movable items that are not attached to land) that occurs during the policy period as a result of, for example, fire, windstorm, explosion, or vandalism.

Protected cell. A structure available to captive insurers underwriting risks of unaffiliated companies whereby the assets associated with the self-insurance program of one organization are segregated to provide legal-recourse protection from creditors of protected cells providing insurance coverage to other organizations.

Quota-share reinsurance. A form of pro rata reinsurance indemnifying the ceding company for a fixed percent of loss on each risk covered in the contract in consideration of the same percentage of the premium paid to the ceding company.

Rebating. Directly or indirectly giving or offering to give any portion of the premium or any other consideration to an insurance buyer as an inducement to purchase or renew the insurance. Rebates are forbidden under most state insurance codes.

Reinsurance. Insurance placed by an underwriter (the ceding company or reinsured) in another company to transfer or reduce the amount of the risk assumed under the original insurance policy (or group of policies).

Reinsurance premium. The consideration paid by a ceding company to a reinsurer for the coverage provided by the reinsurer.

Residual market. Also known as the shared market, it covers applications for insurance that were rejected by underwriters in the voluntary market that is covered by agency direct-marketing systems, perhaps because of high loss experience by the insured party. The residual market includes government insurance programs, specialty pools, and shared market mechanisms such as assigned-risk plans.

Retrocession. A reinsurance transaction whereby a reinsurer (the retrocedant) cedes all or part of the reinsurance risks it has assumed to another reinsurer (the retrocessionaire).

Retrospective rating. An insurance plan in which the current year's premium is based on the insured's own loss experience for that same period, subject to a maximum and minimum.

Rider. A written attachment, also known as an endorsement, to an insurance policy that changes the original policy to meet specific requirements, such as increasing or decreasing benefits or providing coverage for specific property items beyond that provided for under the insurance company's standard contract terms.

Self-insured retention (SIR). The percentage of a risk or potential loss assumed by an insured, whether in the form of a deductible, self-insurance, or no insurance at all.

Separate accounts. Certain life insurance assets and related liabilities that are segregated and maintained to meet specific investment objectives of contract holders, particularly those assets and liabilities associated with pension plans and variable products offered by life insurers, wherein the customer and not the insurer retains most of the investment and interest-rate risk.

Split-dollar life insurance. An arrangement that typically involves an agreement between an employer and an employee whereby the premium payment, cash values, policy ownership, and death benefits may be split. There are many variations of split-dollar arrangements, including arrangements in which a trust is created to facilitate estate planning. Split-dollar life insurance is designed to serve as a supplemental

benefit to a particular company executive. The arrangement typically involves the payment of the insurance premium by the employer, with the death benefit accruing to the employee.

Subrogation. An insurance carrier may reserve the ''right of subrogation'' in the event of a loss. This means that the company may choose to take action to recover the amount of a claim paid to a covered insured if a third party caused the loss. After expenses, the amount recovered must be divided proportionately with the insured to cover any deductible for which the insured was responsible.

Term life insurance. An insurance product that provides, for a specified period of time, death coverage only. Typically, it has no savings component and, therefore, no cash value. Because term insurance provides only mortality protection, it generally provides the most coverage per premium dollar. Most term life insurance policies are renewable for one or more time periods up to a stipulated maximum age; however, premiums generally increase with the age of the policyholder.

Title insurance. Insurance that protects banks and mortgagees against unknown encumbrances against real estate by indemnifying the mortgagor and property owner in the event that clear ownership of the property is clouded by the discovery of faults in the title. Title insurance policies may be issued to either the mortgagor or the mortgagee or both. Title insurance is written largely only by companies specializing in this class of insurance.

Treaty reinsurance. A reinsurance contract under which the reinsured company agrees to cede, and the reinsurer agrees to assume, risks of a particular class or classes of business.

Twisting. In insurance, twisting involves making misrepresentations to a policyholder to induce the policyholder to terminate one policy and take out another policy with another company, when it is not to the insured's benefit. Twisting is a violation of the Unfair Trade Practices Act. Twisting is similar to the ''churning'' concept in securities sales, and it results in increased commissions for the inducing agent.

Umbrella liability insurance. This type of liability insurance provides excess liability protection over the ''underlying'' liability insurance coverage to supplement underlying policies that have been reduced or exhausted by loss.

Underwriting. The process by which a company determines whether it can accept an application for insurance and by which it may charge an appropriate premium for those applications selected. For example, the underwriting process for life insurance classifies applicants by identifying such characteristics as age, sex, health, and occupation.

Unearned reinsurance premium. The part of the reinsurance premium that is applicable to the unexpired portion of the policies reinsured.

Universal life insurance. A form of permanent insurance designed to provide flexibility in premium payments and death benefit protection. The policyholder can pay maximum premiums and maintain a high cash surrender value. Alternatively, the policyholder can make minimal payments in an amount only large enough to cover mortality and other expense charges.

Variable annuity. See *Annuity.*

Variable life insurance. A form of whole life, or universal life, insurance in which the policyholder's cash value is invested in ''separate accounts'' of the insurer. These accounts are segregated from the insurance carrier's other asset holdings. Such separate account investments are generally not available to a carrier's general creditors in the event of the carrier's insolvency. The policyholder assumes the investment and price risk. Because variable life policies have investment features, life insurance agents selling these policies must be registered representatives of a broker-dealer licensed by the Financial Industry Regulatory Authority and registered with the Securities and Exchange Commission.

Vendors' single-interest insurance. A form of force-placed insurance that is typically purchased by the bank to protect against loss or damage to loan collateral in which the bank has a security interest. The bank passes its expense for this insurance on to the consumer who has either refused or is unable to obtain property insurance.

Viatical settlement. The cashing in of a life insurance policy at a discount from face amount

by policyholders who are often terminally ill and need the money for medical care. The purchaser becomes the policyholder as well as the beneficiary and assumes the premium payments of the policy.

Whole life insurance. A fixed-rate insurance product, with premiums and death benefits guaranteed over the duration of the policy. There is a cash value (essentially a savings account) that accrues to the policyholder tax deferred. A policyholder receives the cash value in lieu of death benefits if the policy matures or lapses before the insured's death. A policyholder also may borrow against the policy's accumulated cash value or use it to pay future premiums. For most whole life insurance policies, premiums are constant for the life of the insured's contract.

Insurance Sales Activities and Consumer Protection in Sales of Insurance

Examination Objectives

Effective date November 2003

Section 4043.2

1. To understand the volume and complexity of the state member bank's insurance or annuity program and insurance sales strategy.
2. To assess the financial results of the insurance and annuity sales activity compared with planned results.
3. To determine if the state member bank's insurance and annuity sales activities are effectively integrated into the risk-management, audit, and compliance functions and if the control environment is adequate.
4. To assess the adequacy of the state member bank's controls to ensure compliance with the applicable state and federal laws and regulations.
5. To assess the state member bank's level and direction of operational and legal risks from the insurance or annuity sales activity.

The following objectives apply if insurance products or annuities are sold by a bank or another person at an office of, or on behalf of, the bank.

6. To assess the adequacy of the state member bank's oversight program for ensuring compliance with the Consumer Protection in Sales of Insurance (CPSI) regulation. (See section 4043.1.)
7. To assess the effectiveness of the state member bank's audit and compliance programs for the CPSI regulation.
8. To assess the state member bank's current compliance with the CPSI regulation.
9. To obtain commitments for corrective action when the state member bank is in violation of the CPSI regulation or when applicable policies, procedures, practices, or management oversight to protect against violations is deficient.

RISK ASSESSMENT OF INSURANCE AND ANNUITY SALES ACTIVITIES

The examiner should consider the following procedures, as appropriate, when conducting a risk assessment to determine the level and direction of risk exposure to the state member bank that is attributable to insurance or annuity sales activity. If there are specific areas of concern, the examiner should focus primarily on those areas.

1. *Scope of activities and strategies.* Assess the significance and complexity of the insurance or annuity sales program.
   a. Obtain a general overview of the scope of the state member bank's insurance or annuity sales activities and any anticipated or recent change in or expansion of such activities.
   b. Determine the state member bank's strategy for insurance or annuity sales, including strategies for cross-selling and referrals of insurance and banking products. Determine the institution's experience with any cross-marketing programs for both insurance business generated by the bank and bank business generated by insurance producers.
   c. Obtain two years' worth of income statements, balance sheets, and budget documents for the agency's activities. Compare the expected budget items with their actual results.
   d. Determine the volume and type of insurance or annuity products and services sold or solicited.
   e. Determine what other related services the state member bank provides in connection with its insurance or annuity sales activities, such as providing risk-management services to clients seeking advice on appropriate insurance coverages, claims processing, and other activities.
2. *Insurance sales products and concentrations.*
   a. Determine the composition of sales—
      • by line of business, such as property/casualty insurance, life insurance including annuities, and health insurance;
      • by the proportion of sales to commercial and retail customers; and
      • by the portion of sales that is credit related, such as credit life and credit health insurance.
   b. Determine any sales concentrations to particular entities, industries, or bank customers.
   c. Note any concentrations to large commercial accounts.
   d. Determine what insurance services are provided to the bank, its employees, and bank affiliates.
3. *Legal-entity and risk-management structure for insurance or annuity sales.*
   a. Obtain an organizational chart for the legal-entity and risk-management structure for the insurance or annuity sales activities.
   b. Determine—
      • whether the insurance or annuity sales activity is conducted in an affiliated producer, by the bank itself, through another distribution arrangement, or by a combination of these arrangements;
      • the names of any affiliated insurance agencies and the states where the affiliated insurance agencies are licensed;
      • the locations outside of the United States where insurance or annuities are sold or solicited; and
      • if any subsidiary agency operates as a financial subsidiary under the Gramm-Leach-Bliley Act.
   c. Determine if the insurance or annuity producer is acting as a managing general agent (MGA).[1] If so, determine—
      • the scope of the MGA activities;
      • the state member bank management's assessment of the risk associated with the MGA activity; and

1. MGAs do not assume underwriting risk. Through contractual arrangements with an insurer, MGAs have the authority to write policies on behalf of the insurer in certain instances, thereby binding the insurer to the policy. Certain minimum provisions governing MGA agreements are delineated in the applicable National Association of Insurance Commissioners (NAIC) model law.

- what risk controls are in place to protect the state member bank from potential loss that may arise from the MGA's activities, such as loss arising from legal liability.

4. *Strategic and financial plans.* Assess management controls over the insurance and annuity sales activities.
   a. Ascertain the state member bank management's strategic and financial plans and goals for the insurance or annuity sales activity.
   b. Review the state member bank's due-diligence process for acquiring and pricing agencies, if applicable.
   c. Review the state member bank's financial budgets and forecasts for the activity, particularly plans for new products, marketing strategies and marketing arrangements, and the rate of actual and expected growth for the activity.
   d. Determine the cause for significant deviations from the plan.
   e. Determine if any agency acquired by the state member bank is providing the expected return on investment and if the agency's revenues are covering the debt servicing associated with the purchase, if applicable.
5. *Review of board and committee records and reports.*
   a. Review the reports of any significant state member bank oversight committees, including relevant board of directors and board committee minutes and risk-management reports.
   b. Determine if the board of directors, a board committee, or senior management of the state member bank reviews reports pertaining to consumer complaints and complaint resolution, information pertaining to litigation and associated losses, and performance compared with the organization's plan for the insurance and annuity sales activities.
6. *Policies and procedures.*
   a. Determine—
      - the adequacy of the state member bank's policies and procedures for conducting and monitoring insurance or annuity sales activities, including those policies designed to ensure adherence with federal and state laws and regulations pertaining to consumer protection;
      - whether there are appropriate policies and procedures for the handling of customer funds collected on behalf of the underwriter; accurate and timely financial reporting; complaint monitoring and resolution; effective system security and disaster-recovery plans; and policy-exception tracking and reporting; and
      - if the board of directors or its designated committee has formally approved the policies.
   b. Obtain a detailed balance sheet for agency subsidiaries, and determine if the assets held by insurance or annuity agency subsidiaries of the state member bank are all bank-eligible investments.
   c. Determine the independence of the state member bank's audit program applicable to the insurance and annuity sales activity. Determine if the audit program's scope, frequency, and resources are commensurate with the insurance or annuity sales activities conducted.
   d. Determine how the state member bank selects insurance underwriters with whom to do business, as well as how the state member bank monitors the continuing performance of the underwriters.
   e. Determine the adequacy of the oversight of the bank's board of directors over the insurance management team's qualifications, the training and licensing of personnel, and general compliance with state insurance regulations.
   f. Review the internal controls of the state member bank related to third-party arrangements, including arrangements for sales, processing, and auditing of insurance or annuity sales activities.
7. *Claims, litigation, and functional regulatory supervision.*
   a. Identify any significant litigation against the state member bank arising from its insurance or annuity sales activity and the likely impact of the litigation on the state member bank.
   b. Obtain the insurance agency's errors and omissions claims records for the past several years, including a listing of claims it has made and the amount of claims, the claim status, and the amount of claim payments.

c. Review the state member bank's policies and procedures for tracking and resolving claims. Determine if they appear adequate and if they are adhered to.
d. Determine if the applicable functional regulator has any outstanding supervisory issues with the insurance agency.

8. *Consumer complaints.*
a. Determine if bank management has policies and procedures in place to assess whether consumer complaints received are likely to expose the state member bank to regulatory action, litigation, or other significant risk.
b. Obtain applicable consumer complaint files, and evaluate internal control procedures to ensure the complaints are being adequately addressed.

9. *Audit and compliance functions.*
a. Determine the date of the most recent review of the insurance or annuity sales activities by the audit and compliance functions.
b. Determine the adequacy of the state member bank's management policies and procedures for ensuring that any deficiencies noted in such reviews are corrected, and ascertain whether any such deficiencies are being adequately addressed.[2]

10. *Insurance underwriter oversight of agent/agency activities.*
a. Determine if there are adequate policies and procedures to review and resolve any issues or concerns raised by an insurance underwriter regarding the producers used by, or affiliated with, the state member bank.[3]
b. Determine whether any of the insurance underwriters conducted a periodic review of the producers that they engaged to sell insurance.

11. *State supervisory insurance authorities.*
a. During discussions with state member bank management, determine whether state insurance regulators have raised any issues or concerns in correspondence or reports.
b. Consult with the state insurance regulators, as appropriate, to determine any significant supervisory issues, actions, or investigations. (For multistate agencies, contacts with states may be prioritized on the basis of the location of the agency's head office or by a determination of the significance of sales by state. Both financial examinations and market conduct examinations conducted by the state insurance departments are targeted at insurance underwriters, not agencies. Therefore, information available from the states pertaining to agencies may be very limited.)

12. *Operational risk assessment.* Ascertain from the state member bank's management whether there are—
a. any significant operational problems or concerns relating to insurance or annuity sales activities;
b. policies and procedures in place to ensure accurate and timely reporting to the state member bank's management of insurance or annuity sales activity plans, financial results, and significant consumer complaints or lawsuits or compliance issues, such as errors and omissions claims;[4]
c. appropriate policies and procedures at the state member bank to ensure accurate reporting of insurance or annuity sales activity on Federal Reserve regulatory reports (Determine from applicable Board or Reserve Bank contacts if there are any outstanding issues with respect to potential reporting errors on submitted Federal Reserve reports, bank call reports, or other applicable reports. If so, seek resolution of the issues.); and
d. adequate disaster-recovery plans and procedures to protect the state member bank from loss of data related to insurance or annuity sales activities.

2. Enforcement of the privacy provisions of the Gramm-Leach-Bliley Act as they relate to state member banks is the responsibility of the Board's Division of Consumer and Community Affairs. However, enforcement of the privacy provisions of the GLB Act with respect to the insurance activities of nondepository subsidiaries of a state member bank is the responsibility of the state insurance regulators.

3. Insurance underwriters generally have procedures to determine whether individual producers affiliated with agencies are selling the underwriters' products in conformance with applicable laws and regulations. The findings and conclusions of these reviews should be available to the state member bank's management.

4. Errors and omissions insurance should be in place to protect the state member bank against loss sustained because of an error or oversight, such as failure to issue an insurance policy. A tracking system to monitor errors and omission claims should be in place and monitored by the state member bank, as appropriate. See section 4040.1, "Management of Insurable Risks."

CONSUMER PROTECTION IN SALES OF INSURANCE REGULATION

The following procedures should be risk-focused in accordance with the Federal Reserve's risk-focused framework for supervising banking organizations. The procedures should be carried out as necessary to adequately assess the state member bank's compliance with the Consumer Protection in Sales of Insurance (CPSI) regulation.

1. Determine the role of the state member bank's board of directors and management in ensuring compliance with the CPSI regulation and applicable state consumer regulations.
2. Evaluate the management information system (MIS) reports the state member bank's board or designated committee rely on to monitor compliance with the consumer regulations and to track complaints and complaint resolution.
3. Review the state member bank's policies and procedures to ensure they are consistent with the CPSI regulation, and conduct transaction testing, as necessary, in the following areas.[5]
   a. disclosures, advertising, and promotional materials
   b. consumer acknowledgments
   c. physical separation from areas of deposit-taking activities
   d. qualifications and licensing for insurance personnel
   e. compliance programs and internal audits
   f. hiring, training, and supervision of insurance or annuity sales personnel employed directly by the bank, or of third parties selling insurance or annuity products at a state member bank office or on behalf of the state member bank
   g. compensation practices and training for personnel making referrals
4. If a third party sells insurance or annuities at the state member bank's offices, or on behalf of the bank, review the state member bank's policies and procedures for ensuring that the third party complies with the CPSI regulation and other relevant policies and procedures of the bank.
5. Review the bank's process for identifying and resolving consumer complaints related to the sale of insurance products and annuities.
6. Obtain and review the record of consumer complaints related to the CPSI regulation. These records are available from the Board's Division of Consumer and Community Affairs database. (See CP letter 2001-11.)
7. Include examination findings, as appropriate, in the commercial bank examination report or in other communications to the bank, as appropriate, that pertain to safety-and-soundness reviews of the bank.

5. If the examiner determines that transaction testing of a functionally regulated nonbank affiliate of the state member bank is appropriate in order to determine the state member bank's compliance with the CPSI regulation, the examiner should first consult with and obtain approval from appropriate staff of the Board's Division of Banking Supervision and Regulation.

Insurance Sales Activities and Consumer Protection in Sales of Insurance

Internal Control Questionnaire

Effective date November 2003

Section 4043.4

RISK ASSESSMENT OF INSURANCE AND ANNUITY SALES ACTIVITIES

Program Management

1. Does the state member bank have a comprehensive program to ensure that its insurance and annuity sales activities are conducted in a safe and sound manner?
2. Does the state member bank have appropriate written policies and procedures commensurate with the volume and complexity of the insurance or annuity sales activities?
3. Has bank management obtained the approval of the bank's board of directors for the program scope and the associated policies and procedures?
4. Have reasonable precautions been taken to ensure that disclosures to customers for insurance or annuity sales and solicitations are complete and accurate, and are in compliance with applicable laws and regulations?
5. Does the state member bank effectively oversee the insurance or annuity sales activities, including those involving third parties?
6. Does the state member bank have an effective independent internal audit and compliance program in place to monitor retail sales of insurance or annuity products?
7. Does the bank appropriately train and supervise employees conducting insurance or annuity sales activities?

Management Information Systems

8. Does the state member bank's insurance program management plan establish the appropriate management information systems (MIS) necessary for the board of directors to properly oversee the bank's insurance or annuity sales activities?
9. Does MIS provide sufficient information to allow for the evaluation and measurement of the effect of actions taken to identify, track, and resolve any issues relative to compliance with the Consumer Protection in Sales of Insurance (CPSI) regulation?
10. Does MIS include sales volumes and trends, profitability, policy exceptions and associated controls, customer complaints, and other information providing evidence of compliance with laws and established policies?

Compliance Programs and Internal Audits

11. Are there policies and procedures in place to ensure that insurance or annuity sales activities are conducted in compliance with applicable laws and regulations?
12. Do compliance procedures identify potential conflicts of interest and how such conflicts should be addressed?
13. Do the compliance procedures provide a system to monitor customer complaints and track their resolution?
14. When applicable, do compliance procedures call for verification that third-party sales are being conducted in a manner consistent with the agreement governing the third party's arrangement with the state member bank?
15. Is the compliance function conducted independently of the insurance or annuity sales and management activities?
16. Do compliance personnel determine the scope and frequency of the insurance-product review?
17. Are findings of insurance or annuity sales activity compliance reviews periodically reported directly to the state member bank's board of directors or a designated committee thereof?

CONSUMER PROTECTION IN SALES OF INSURANCE REGULATION

If applicable, review the state member bank's internal controls, policies, practices, and procedures for retail insurance or annuity sales activi-

ties conducted by the bank on bank premises or on behalf of the bank. The bank's program management for such activities should be well documented and should include appropriate personnel training, as well as compliance and audit-function coverage of all efforts to ensure compliance with the provisions of the Board's CPSI regulation.

Advertising and Promotional Materials

1. Do advertising materials associated with the insurance or annuity sales program create an erroneous belief that—
   a. an insurance product or annuity sold or offered for sale by the state member bank, or on behalf of the bank, is backed by the federal government or the bank, or that the product is insured by the FDIC?
   b. an insurance product or annuity that involves investment risk does not, in fact, have investment risk, including the potential that principal may be lost and the product may decline in value?
2. Does a review of advertising for insurance products or annuities sold or offered for sale create an erroneous impression that—
   a. the state member bank or an affiliate or subsidiary may condition the grant of an extension of credit to a consumer on the purchase of an insurance product or annuity by the consumer from the bank or an affiliate or subsidiary of the bank?
   b. the consumer is not free to purchase an insurance product or annuity from another source?

Disclosures

3. In connection with the initial purchase of an insurance product or annuity by a consumer, does the initial disclosure to the consumer, except to the extent the disclosure would not be accurate, state that—
   a. the insurance product or annuity is not a deposit or other obligation of, or is not guaranteed by, the state member bank or an affiliate of the bank?
   b. the insurance product or annuity is not insured by the FDIC or any other agency of the United States, the state member bank, or (if applicable) an affiliate of the bank?
   c. in the case of an insurance product or annuity that involves an investment risk, there is risk associated with the product, including the possible loss of value?
4. In the case of an application for credit, in connection with which an insurance product or annuity is solicited, offered, or sold, is a disclosure made that the state member bank may not condition an extension of credit on either—
   a. the consumer's purchase of an insurance product or annuity from the bank or any of its affiliates?
   b. the consumer's agreement not to obtain, or a prohibition on the consumer's obtaining, an insurance product or annuity from an unaffiliated entity?
5. Are the disclosures under question 3 above provided orally and in writing before the completion of the initial face-to-face sale of an insurance product or annuity to a consumer?
6. Are the disclosures under question 4 above made orally and in writing at the time the consumer applies in a face-to-face interaction for an extension of credit in connection with which insurance is solicited, offered, or sold?
7. If a sale of an insurance product or annuity is conducted by telephone, are the disclosures under question 3 above provided in writing, by mail, within three business days?
8. If an application for credit is by telephone, are the disclosures under question 4 above provided by mail to the consumer within three business days?
9. Are the disclosures under questions 3 and 4 above provided through electronic media, instead of on paper, only if the consumer affirmatively consents to receiving the disclosures electronically, and only if the disclosures are provided in a format that the consumer may retain or obtain later?
10. Are disclosures made through electronic media, for which paper or oral disclosures are not required, presented in a meaningful form and format?
11. Are disclosures conspicuous, simple, direct, readily understandable, and designed to call attention to the nature and significance of the information provided?
12. Are required disclosures presented in a meaningful form and format?

Consumer Acknowledgment

13. At the time a consumer receives the required disclosures, or at the time of the consumer's initial purchase of an insurance product or annuity, is a written acknowledgment from the consumer that affirms receipt of the disclosures obtained?
14. If the required disclosures are provided in connection with a transaction that is conducted by telephone—
    a. has an oral acknowledgment of receipt of the disclosures been obtained, and is sufficient documentation maintained to show that the acknowledgment was given?
    b. have reasonable efforts to obtain a written acknowledgment from the consumer been made?

Physical Separation from Deposit Activities

15. Does the state member bank, to the extent practicable—
    a. keep the area where the bank conducts transactions involving the retail sale of insurance products or annuities physically segregated from the areas where retail deposits are routinely accepted from the general public?
    b. identify the areas where insurance product or annuity sales activities occur?
    c. clearly delineate and distinguish insurance and annuity sales areas from the areas where the bank's retail deposit-taking activities occur?

Qualifications and Licensing

16. Does the state member bank permit any person to sell, or offer for sale, any insurance product or annuity in any part of its office, or on its behalf, only if the person is at all times appropriately qualified and licensed under applicable state insurance licensing standards for the specific products being sold or recommended?

Hiring, Training, and Supervision

17. Have background investigations of prospective employees that will sell insurance products or annuities been completed?
18. When a candidate for employment has previous insurance experience, has a review to determine whether the individual has been the subject of any disciplinary actions by state insurance regulators been completed?
19. Do all insurance or annuity sales personnel, or third-party sales personnel conducting sales activities at or on behalf of the state member bank, receive appropriate training and continue to meet licensing requirements?
20. Does training address policies and procedures for sales of insurance and annuity products, and does it cover personnel making referrals to a licensed insurance producer?
21. Does training ensure that personnel making referrals about insurance products or annuities are properly handling all inquiries so as not to be deemed to be acting as unlicensed insurance agents or registered (or equivalently trained) securities sales representatives (for insurance products that are also securities) if they are not qualified?
22. When insurance products or annuities are sold by the state member bank or third parties at an office of, or on behalf of, the organization, does the institution have policies and procedures to designate, by title or name, the individuals responsible for supervising insurance sales activities, as well as the referral activities of bank employees not authorized to sell these products?
23. Does the bank designate supervisory personnel responsible for monitoring compliance with any third-party agreement, as well as with the CPSI regulation?

Referrals

24. Are fees paid to nonlicensed personnel who are making referrals to qualified insurance or annuity salespersons limited to a one-time, nominal fee of a fixed dollar amount for each referral, and is the fee unrelated to whether the referral results in a sales transaction?

Third-Party Agreements

25. Does the state member bank's management conduct a comprehensive review of a third party before entering into any arrangement to conduct insurance or annuity sales activities through the third party?
26. Does the review include an assessment of the third party's financial condition, management experience, and ability to fulfill its contractual obligations to the bank, including compliance with applicable consumer protection laws and regulation?
27. Does the board of directors or a designated committee thereof approve any agreement with the third party?
28. Does the agreement outline the duties and responsibilities of each party; describe the third-party activities permitted on the institution's premises; address the sharing or use of confidential customer information; and define the terms for use of the bank's office space, equipment, and personnel?
29. Does the third-party agreement specify that the third party will comply with all applicable laws and regulations and will conduct its activities in a manner consistent with the CPSI regulation, if applicable?
30. Does the agreement authorize the bank to monitor a third party's compliance with the agreement, as well as to have access to third-party records considered necessary to evaluate compliance?
31. Does the agreement provide for indemnification of the institution by the third party for any losses caused by the conduct of the third party's employees in connection with its insurance or annuity sales activities?
32. If an arrangement includes dual employees, does the agreement provide for written employment contracts that specify the duties of these employees and their compensation arrangements?
33. If the state member bank contracts with a functionally regulated third party, does the bank obtain, as appropriate, any relevant regulatory reports of examination of the third party?
34. How does the state member bank ensure that a third party selling insurance or annuity products at or on behalf of the bank complies with all applicable regulations, including the CPSI regulation?
35. How does the state member bank ensure that any third party or dual employee selling insurance or annuity products at or on behalf of the bank is appropriately trained to comply with the minimum disclosures and other requirements of the Board's CPSI regulation and applicable state regulations?
36. Does the bank obtain and review copies of third-party training and compliance materials to monitor the third party's performance regarding its disclosure and training obligations?

Consumer Complaints

37. Does the state member bank have policies and procedures for handling customer complaints related to insurance and annuity sales?
38. Does the customer complaint process provide for the recording and tracking of all complaints?
39. Does the state member bank require periodic reviews of complaints by compliance personnel? Is a review by the state member bank's board and senior management required for significant compliance issues that may pose risk to the state member bank?

INTRODUCTION

Banks routinely rely on third parties for a range of products, services, and other activities. The use of third parties can offer banks efficient access to technologies, human capital, delivery channels, products, services, and markets. As a result, the numbers and types of banks' third-party relationships have increased over time. The use of third parties, especially those utilizing new technologies, may present elevated risks to a bank and its customers, including operational, compliance, and strategic risks. Therefore, when a bank uses a third party, the bank needs a strong risk-management process to ensure that the third party conducts its activities in a safe-and-sound manner and in compliance with applicable laws and regulations. Such laws and regulations include those designed to protect consumers (i.e., fair lending laws and prohibitions against unfair, deceptive, or abusive acts or practices) and those addressing financial crimes.

The purpose of this manual section is to provide a summary of *Interagency Guidance on Third-Party Relationships* (interagency guidance) issued by the Federal Reserve, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency (collectively, the agencies) on managing risks associated with third-party relationships. For the complete guidance see SR-23-4, "Interagency Guidance on Third-Party Relationships: Risk Management."[1]

INTERAGENCY GUIDANCE ON MANAGING RISKS ASSOCIATED WITH THIRD-PARTY RELATIONSHIPS

Overview

The agencies issued the interagency guidance to assist banks in identifying and managing risks associated with third-party relationships and in complying with applicable laws and regulations.[2] Furthermore, the interagency guidance offers the agencies' views on sound risk-management principles for supervised institutions when developing and implementing risk-management practices for all stages in the life cycle of third-party relationships. In the end, a bank's third-party risk management should reflect the level of risk, complexity, and size of the bank and the nature of its third-party relationship.

Applicability of the Guidance

The interagency guidance is relevant to institutions supervised by the agencies. For the Federal Reserve, this primarily includes state member banks, bank holding companies, savings and loan holding companies, U.S. branches and agencies of foreign banking organizations, and Edge Act and agreement corporations.

The interagency guidance addresses any business arrangement between a bank and a third-party entity, by contract or otherwise. A "business arrangement" is another term for "third-party relationship," including

- outsourced services,
- independent consultants,
- referral arrangements,
- merchant payment processing services,
- services provided by affiliates and subsidiaries, and
- joint ventures.

Risk Management

As a third-party relationship presents a varying level of risk, a bank's risk-management practices should include

- analyzing the risks associated with each third-party relationship;
- tailoring risk-management practices, commensurate with the bank's size, complexity, and risk profile as well as the nature of the third-party relationship;

1. See also 88 Fed. Reg. 37,920 (June 9, 2023).
2. These include the "Interagency Guidelines Establishing Standards for Safety and Soundness," and the "Interagency Guidelines Establishing Information Security Standards," which were adopted pursuant to the procedures of section 39 of the Federal Deposit Insurance Act and section 505 of the Graham Leach Bliley Act, respectively. See 12 CFR pt. 208, appendices D-1 and D-2.

- maintaining a complete inventory of its third-party relationships;
- periodically conducting risk assessments for each third-party relationship and determining whether risks have changed over time and risk-management practices need to be updated; and
- engaging in more rigorous oversight and management of third-party relationships that support higher-risk activities, including the bank's critical activities.

Critical Activities

Critical activities will depend upon a bank's risk profile and business operations. Characteristics of critical activities may include those activities that could

- cause a bank to face significant risk if the third party fails to meet expectations;
- have significant customer impacts; or
- have a significant impact on a bank's financial condition or operations.

A bank should identify its critical activities and third-party relationships that support these activities. Some banks may assign a criticality or risk level to each third-party relationship, whereas others identify critical activities and those third parties that support such activities.

Third-Party Relationship Life Cycle

Effective third-party risk management generally follows a continuous life cycle for third-party relationships. The stages of the risk-management life cycle of third-party relationships are shown in figure 1 and detailed below. The interagency guidance includes examples of risk-management practices that a bank may find helpful in the development and maintenance of its risk-management process. However, these examples may not apply to all banks' third-party relationships.

Bank staff with the requisite knowledge and skills should appropriately implement each stage of the risk-management life cycle. A bank may involve experts across disciplines, such as compliance, risk, or technology as well as legal counsel, and may engage external support when helpful to supplement the qualifications and technical expertise of in-house staff.[3]

Figure 1. The risk-management life cycle of third-party relationships

Planning

As part of sound risk management, effective planning allows a bank to evaluate and consider its approach for managing risks before entering into a third-party relationship. Certain third parties, such as those that support a bank's higher-risk activities, including critical activities, typically warrant a greater degree of planning and consideration. For example, when critical activities are involved, plans may be presented to and approved by a bank's board of directors (or a designated board committee).

Due Diligence and Third-Party Selection

Conducting due diligence on third parties before selecting and entering into third-party relationships is an important part of sound risk management. Due diligence includes assessing the third party's ability to perform the activity as expected, adhere to a bank's policies related to the activity, comply with all applicable laws and regulations, and conduct the activity in a safe and sound manner. The due diligence process provides

- management with the information needed about potential third parties to determine if a

3. When a bank uses a third-party assessment service or utility, it has a business arrangement with that entity. Therefore, the arrangement should be incorporated into the bank's third-party risk-management processes.

relationship would help achieve a bank's strategic and financial goals; and
- the bank with the information needed to evaluate whether it can appropriately identify, monitor, and control risks associated with the particular third-party relationship.

Relying solely on experience with or prior knowledge of a third party is not an adequate proxy for performing appropriate due diligence, as the scope and degree of due diligence should be commensurate with the level of risk and complexity of the third-party relationship.[4]

Contract Negotiation

When evaluating whether to enter into a relationship with a third party, a bank typically determines whether a written contract is needed, and if the proposed contract can meet its business goals and risk-management needs. After such determination, a bank typically negotiates contract provisions that will facilitate effective risk management and oversight and that specify the expectations and obligations of both the bank and the third party. A bank may tailor the level of detail and comprehensiveness of such contract provisions based on the risk and complexity posed by the particular third-party relationship.

Ongoing Monitoring

Ongoing monitoring enables a bank to (1) confirm the quality and sustainability of a third party's controls and ability to meet contractual obligations; (2) escalate significant issues or concerns, such as material or repeat audit findings, deterioration in financial condition, security breaches, data loss, service interruptions, compliance lapses, or other indicators of increased risk; and (3) respond to such significant issues or concerns when identified.

Typical monitoring activities include:

1. Reviewing reports regarding the third party's performance and the effectiveness;
2. Periodically visiting and meeting with third-party representatives; and
3. Regularly testing a bank's controls that manage risks from its third-party relationships.

Table 1 provides information on a bank's risk management of third-party relationships, focusing on due diligence, contract negotiations, and ongoing monitoring considerations.

Termination

A bank may terminate a relationship for various reasons, such as expiration or breach of the contract; the third party's failure to comply with applicable laws or regulations; or a desire to seek an alternate third party, bring the activity in-house, or discontinue the activity. In terminating a relationship, bank management should consider whether the activities will be transitioned to another third party, brought in-house, or discontinued. Depending on the degree of risk and complexity of the third-party relationship, a bank typically considers various factors to facilitate termination such as

- transitioning services and activities.
- costs and fees associated with termination.
- managing risks associated
  - with data retention and destruction;
  - information system connections and access control, or other control concerns;
  - handling of joint intellectual property; and
  - with the termination of services including any impact on customers and the necessary action to address the third party's inability to perform in accordance with service expectations.

Governance

Oversight and Accountability

Proper oversight and accountability in the third-party risk-management process aid a bank in minimizing adverse financial, operational, or other consequences. A bank's board of directors has ultimate responsibility for providing oversight for third-party risk management and holding bank management accountable. The board also provides clear guidance regarding acceptable risk appetite, approves appropriate policies, and ensures that appropriate procedures and

4. For more background information, see *Community Bank Access to Innovation Through Partnerships* (September 2021) and *Interagency Due Diligence Guide for Community Banks* (August 2021).

practices have been established. In turn, bank management is responsible for developing and implementing third-party risk-management policies, procedures, and practices, commensurate with the bank's risk appetite and the level of risk and complexity of its third-party relationships. Table 2 highlights the typical roles and responsibilities of a bank's board and management in the third-party risk-management process.

Independent Reviews

Periodic independent reviews of third-party relationships allow a bank to assess the adequacy of its risk-management processes over third-party activities. Such reviews typically consider whether

- the third-party relationships align with the bank's business strategy, and with internal policies, procedures, and standards;
- risks of third-party relationships are identified, measured, monitored, and controlled;
- the bank's processes and controls are designed and operating adequately;
- the bank's staff with appropriate expertise are engaged to perform risk-management activities throughout the third-party risk-management life cycle; and
- conflicts of interest or appearances of conflicts of interest are avoided or eliminated when a bank selects a third party and as part of its oversight process for monitoring the activities of third parties.

The results of independent reviews may aid a bank in determining whether and how to adjust its third-party risk-management process, including its policies, reporting, resources, expertise, and controls. Furthermore, bank management should respond promptly and thoroughly to issues or concerns identified and escalate them to the bank's board of directors, as appropriate.

Documentation and Reporting

Documentation and reporting are key elements of a bank's risk-management process for overseeing third-party risk activities and the activities of specific third-party relationships throughout the life cycle of that relationship. The extent of documentation and reporting will depend on the complexity of a bank's third-party relationships. The following are examples of processes that support effective documentation and internal reporting:

- a current inventory of all third-party relationships (and, as appropriate, related subcontractors) that clearly identifies higher-risk and critical activities;
- planning and risk assessments related to the use of third parties;
- due diligence results and recommendations;
- executed contracts;
- results of independent reviews;
- remediation plans and related reports addressing the quality and sustainability of the third party's controls;
- risk and performance reports required and received from the third party as part of ongoing monitoring;
- if applicable, reports related to customer complaints and inquiry monitoring, and any subsequent remediation reports;
- reports from third parties of service disruptions, security breaches, or other events that pose, or may pose, a material risk to the bank; and
- periodic reporting to the board of directors (including, as applicable, dependency on a single provider for multiple activities).

Supervisory Review of Third-Party Relationships

The Federal Reserve reviews its supervised institutions' risk management of third-party relationships as part of its supervisory processes, tailored to the institution's asset size and complexity. Supervisory reviews will evaluate risks and the effectiveness of risk management to determine whether activities are conducted in a safe-and-sound manner and in compliance with applicable laws and regulations.

In evaluating a bank's third-party risk management, examiners consider whether the bank engages in a diverse set of third-party relationships, recognizing that not all third-party risk relationships present the same risks, and that a bank accordingly tailors its practices to the risks. Thus, the scope of the supervisory review depends on the degree of risk and the complexity associated with a bank's activities and third-party relationships. When reviewing third-party risk-management processes, examiners typically conduct the following activities, among others:

- assess the ability of the bank's management to oversee and manage the bank's third-party relationships;
- assess the impact of third-party relationships on the bank's risk profile and key aspects of financial and operational performance, including compliance with applicable laws and regulations;
- perform transaction testing or review results of testing to evaluate third-party activities and assess compliance with applicable laws and regulations;
- highlight and discuss any material risks and deficiencies in the bank's risk-management process with senior management and the board of directors, as appropriate;
- review the bank's plans for appropriate and sustainable remediation of any deficiencies, particularly those associated with the oversight of third parties that involve critical activities; and
- consider supervisory findings when assigning the components of the applicable rating system and highlight any material risks and deficiencies in the report of examination or supervisory letter.

When circumstances warrant, the Federal Reserve may use its legal authority to examine functions or operations that a third party performs on behalf of a bank. Such examinations may evaluate the third party's ability to fulfill its obligations in a safe-and-sound manner and comply with applicable laws and regulations, including those designed to protect customers and to provide fair access to financial services. The Federal Reserve may pursue corrective measures, including enforcement actions, when necessary to address violations of laws and regulations or unsafe or unsound banking practices by the bank or its third party.

Table 1. Bank risk management of third-party relationships

Risk-management theme	**Due diligence considerations** *The bank should consider the third party's…*	**Contract considerations** *Effective contracts typically discuss…*	**Ongoing monitoring** *The bank should assess…*
Strategies and goals	• Current and proposed strategic business arrangements. • Service philosophies, quality initiatives, and employment policies and practices.	• The nature and scope of the business arrangement. • The activities the third party will perform. • Ancillary services, such as software, technology support, maintenance, and customer service. • Terms governing the use of the bank's information, facilities, personnel, systems, intellectual property, and equipment as well as the bank's or customers' information. • All costs and compensation arrangements.	Changes to the third party's business strategy that may pose new or increased risks or impact the third party's ability to meet contractual obligations.
Legal and regulatory compliance	• Ownership structure. • Whether the third party is subject to sanctions. • Expertise, processes, and controls to enable the bank to comply with applicable laws and regulations. • Responsiveness to issues. • Process to mitigate, areas of potential consumer harm.	The obligations of the third party and the bank to comply with applicable laws and regulations.	The third party's ongoing compliance with applicable laws and regulations and its performance as measured against contractual obligations.
Financial condition	• Audited financial statements, annual reports, and filings with the U.S. Securities and Exchange Commission.	The type and frequency of reports to be received from the third party, including performance reports, financial reports, security reports, and control assessments.	Changes in the third party's financial condition, including its financial obligations to others.
Business experience	• Depth of resources (including staffing). • Previous experience. • History of addressing customer complaints.	The terms governing the use of the bank's personnel. If dual employees will be used, it may also be helpful to specify their responsibilities and reporting lines.	Changes in the third party's key personnel involved in the activity.

Risk-management theme	**Due diligence considerations** *The bank should consider the third party's…*	**Contract considerations** *Effective contracts typically discuss…*	**Ongoing monitoring** *The bank should assess…*
Qualifications and backgrounds of key personnel and other human resources considerations	• Background checks on the third party's key personnel and contractors. • Ability to identify and remove employees failing to meet suitability requirements. • Succession and redundancy planning.	Performance measures that do not incentivize imprudent performance or behavior, such as encouraging processing volume or speed without regard for accuracy, compliance requirements, or adverse effects on the bank or customer.	Training provided to employees of the bank and the third party.
Risk management	• Policies, processes, and internal controls. • Alignment with applicable policies and expectations of the bank surrounding the activity. • Audit assessments, including independent testing and objective reporting of results and findings. • System and Organization Control (SOC) reports.	Provisions for periodic, independent audits of the third party and its relevant subcontractors, consistent with the risk and complexity of the third-party relationship.	Relevant audits, testing results, and other reports that address whether the third party remains capable of managing risks and meeting contractual obligations and regulatory requirements.
Information security	• Information security program and determine whether there are any gaps that present risk. • Experience in identifying, assessing, and mitigating, known and emerging threats and vulnerabilities.	When and how the third party will disclose, in a timely manner, information security breaches or unauthorized intrusions.	The third party's response to changing threats, new vulnerabilities, and incidents impacting the activity, including any resulting adjustments to the third party's operations or controls.
Management information systems	• Ability to identify gaps in service-level expectations, business process and management, and interoperability issues. • Processes for maintaining timely and accurate inventories of its technology and its contractor(s).	• Prohibitions on the use and disclosure of bank and customer information by a third party and its subcontractors, except as necessary to provide the contracted activities or comply with legal requirements. • Obligations for retention and provision of timely, accurate, and comprehensive information.	The third party's ability to maintain the confidentiality, availability, and integrity of the bank's systems, information, and data, as well as customer data, where applicable.

Risk-management theme	**Due diligence considerations** *The bank should consider the third party's…*	**Contract considerations** *Effective contracts typically discuss…*	**Ongoing monitoring** *The bank should assess…*
Operational resilience	• Results from operational resilience and business continuity testing and performance during actual disruptions. • Telecommunications redundancy and resilience plans. • Preparations for threats and vulnerabilities, such as natural disasters, pandemics, distributed denial of service attacks, or other intentional or unintentional events.	The continuation of the activity in the event of problems affecting the third party's operations, including degradations or interruptions in delivery.	The third party's response to incidents, business continuity and resumption plans, and testing results to evaluate the third party's ability to respond to and recover from service disruptions or degradations.
Incident reporting and management processes	Documented processes, timelines, and accountability for identifying, reporting, investigating, and escalating incidents.	Whether the bank or the third party is responsible for responding to customer complaints or inquiries.	The volume, nature, and trends of customer inquiries and complaints, the adequacy of the third party's responses (if responsible for handling customer inquiries or complaints), and any resulting remediation.
Physical security	Physical and environmental controls to protect the safety and security of people, facilities, technology systems, and data, as applicable.	The terms governing the use of the bank's facilities, personnel, systems, and equipment.	*See ongoing monitoring for "Operational resilience" above.*
Reliance on subcontractors	Ability to identify, manage, and mitigate risks associated with subcontracting, including how the third party selects and oversees its subcontractors and ensures that its subcontractors implement effective controls.	When and how the third party should notify the bank of its use or intent to use a subcontractor and whether specific subcontractors are prohibited by the bank.	The third party's reliance on, exposure to, and use of subcontractors, the location of subcontractors (and any related data), and the third party's own risk-management processes for monitoring subcontractors.

Risk-management theme	**Due diligence considerations** *The bank should consider the third party's…*	**Contract considerations** *Effective contracts typically discuss…*	**Ongoing monitoring** *The bank should assess…*
Insurance coverage	Insurance policies and the extent to which potential losses are mitigated, including losses posed by the third party to the bank.	• Specified types and amounts of insurance (including, if appropriate, naming the bank as insured or additional insured). • Notifications to the bank of material changes to coverage. • Expectations for evidence of coverage, as appropriate.	Changes to, or lapses in, the third party's insurance coverage.
Contractual agreements with other parties	Legally binding arrangements with subcontractors or other parties to determine whether such arrangements may create or transfer risks to the bank or its customers.	• Indemnification clauses specifying the extent to which the bank will be held liable for claims or be reimbursed for damages based on the failure of the third party or its subcontractor to perform. • The dispute resolution process to resolve problems between the bank and the third party in an expeditious manner, and whether the third party should continue to provide activities to the bank during the dispute resolution period. • The extent to which the third party has the right to use the bank's information, technology, and intellectual property, such as the bank's name, logo, trademark, and copyrighted material.	Changes to the third party's agreements with other entities that may pose new or increased risks or impact the third party's ability to meet contractual obligations.

Table 2. Third-party risk-management responsibilities for a bank's board of directors and management

Board of directors (or a designated board committee)	Bank management
• Assessing whether third-party relationships are managed in a manner consistent with the bank's strategic goals and risk appetite and in compliance with applicable laws and regulations • Assessing whether there is appropriate periodic reporting on third-party relationships to monitor third-party relationships and these activities • Determining whether management has taken appropriate actions to remedy performance issues and address changing risks or material issues	• Integrating third-party risk management with the bank's overall risk-management processes • Directing the planning, due diligence, and ongoing monitoring of third-party activities • Reporting periodically on third-party activities to the board (or designated board committee) • Providing that contracts with third parties are appropriately reviewed, approved, and executed • Establishing appropriate organizational structures and staffing to oversee third-party activities • Implementing and maintaining an appropriate system of internal controls to manage risks associated with third-party relationships • Assessing whether the bank's compliance management system is appropriate given the nature, size, complexity, and scope of its third-party relationships • Determining whether the bank has appropriate access to data and information from its third parties • Escalating significant issues to the board and monitoring any resulting remediation, including actions taken by the third party • Appropriately terminating business arrangements with third parties

LITIGATION AND OTHER LEGAL MATTERS

Events or conditions arising from litigation,[1] claims, and assessments are matters within the direct knowledge and, often, control of bank management. Accordingly, management is the primary source of information about these matters.[2] Examiners ordinarily do not possess legal skills and therefore cannot make legal judgments on such information.[3] Examiners should request that bank management send a letter of inquiry to those attorneys with whom it has consulted on litigation, claims, and assessments. The letter of inquiry is the examiner's primary means of corroborating information furnished by management.

When requesting these inquiries, examiners should consider the scope of counsel's involvement with the bank. Banks may engage a number of law firms, so examiners should have the bank direct requests to both general counsel and counsel whose service is limited to particular matters. Ordinarily, inquiries should be made of all outside counsel.

In certain instances, however, examiners may be reasonably certain that some of the bank's counsels are handling only routine matters that ultimately will not have a significant effect on the bank's financial condition. In these cases, the examiner-in-charge may decide not to send letters of inquiry to those counsels.

Requests for corroboration from legal counsel should ask for information about litigation, impending litigation, claims, and contingent liabilities. For the purposes of these requests, the terms impending litigation and contingent liabilities have the following meanings:

- *Impending litigation.* Litigation threatened against the bank by a third party but not formally commenced.

- *Contingent liabilities.* Matters other than litigation or claims, which available information indicates have at least a reasonable possibility of impairing assets or increasing liabilities. Contingent liabilities should include unasserted claims or assessments.

A letter of inquiry should ask for a response both as of the examination date and as of the date of counsel's response. That date of response should be as close to the completion of the examination as practicable, yet should allow sufficient time for evaluation of responses and follow-up of nonreplies. In some cases, the examiner may wish to obtain an interim response (in addition to a final response) so that a timely preliminary evaluation of material legal matters may be made. Letters of inquiry should be sent early enough to allow them to circulate within the law firm because several attorneys may be considering legal matters for the bank. Before completing the examination, examiners should request that appropriate bank officials contact counsel who have not responded to the initial letter of inquiry.

If examination staff have reason to believe that there may be subsequent developments, the examiner should contact bank management again before submitting the report of examination. If bank management is uncooperative or regarded as incapable of supervising matters concerning litigation, or if other sensitivities mandate circumvention of bank management, then examiners should bring the matter to the attention of Federal Reserve Bank management for further communications with the bank's management and counsel, which could include direct contact with bank counsel.

EXAMINATION-RELATED SUBSEQUENT EVENTS

As a practical matter, the examination, and therefore the report of examination, is as of a stated date. However, events or transactions sometimes occur, subsequent to the date of examination, but before the date the report of

1. Legal risk arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a financial institution.

2. In limited circumstances, a bank director who is not an officer of the bank may have direct knowledge and control of legal information, usually when the director's primary occupation is as an attorney. Management in these rare instances may have limited knowledge and control of legal information.

3. Appropriate examination staff should notify the enforcement section of Board Legal of any investigations or other legal actions being conducted by governmental regulators or criminal prosecutors against the bank when such information is ascertained during the examination process.

examination is submitted to the Reserve Bank, that may have a significant effect on the soundness of a bank. Such events and transactions are referred to as ''subsequent events'' and may be of two types.

One type includes those events or transactions that provide additional evidence about conditions that existed at the examination date. Examples of this type are the bankruptcy of a significant borrower or the resolution of outstanding litigation.

The second type includes those events that provide evidence about conditions that did not exist at the date of examination but that arose subsequently. An example of that type of event would be new litigation arising subsequent to the examination date but before submission of the examination report.

All information that becomes available before the submission of the report of examination should be used by examiners in the evaluation of the bank. Accordingly, all events or transactions that either significantly affect or have the potential to significantly affect the soundness of the bank should be reflected in the report of examination, regardless of whether they occurred before or subsequent to the examination date.

Litigation and Other Legal Matters, and Examination-Related Subsequent Events

Examination Objectives

Effective date October 2018

Section 4070.2

1. To determine whether any events or transactions have occurred subsequent to the examination date that have had or may have a significant impact on the present or future soundness of the bank or on the conclusions expressed in the report of examination.
2. To determine the adequacy of risk management practices surrounding litigation and other legal matters.
3. To determine the effect of legal counsel's evaluation of litigation, impending litigation, claims, and contingent liabilities on the examiner's overall conclusion regarding the soundness of the bank.

1. Read minutes of all meetings of stockholders, directors, and appropriate committees (investment, loans, etc.).
   a. Ascertain from officials of the bank whether minutes of all such meetings subsequent to the examination date are set forth in the minute book.
   b. As to meetings for which minutes have not been prepared at the date of the review, inquire directly of persons present at the meetings and, preferably, of the person charged with the responsibility of preparing the minutes, concerning matters dealt with at such meetings.
2. If specific violations of law or areas of weakness have been reported to management earlier in the examination, determine the extent to which management has proceeded toward corrective action.
3. Obtain from the bank officer responsible for legal matters a listing of impending or threatened litigation. For each item, the following information should be included:
   a. nature of the litigation
   b. progress of case to date
   c. how management is responding or intends to respond to the litigation
   d. an evaluation of the likelihood of an unfavorable outcome and an estimate, if one can be made, of the amount or range of potential loss
4. Obtain from the bank officer responsible for legal matters a listing of unasserted claims or assessments management considers will probably be asserted and which, if asserted, would have at least a reasonable possibility of an unfavorable outcome. For each item, the following information should be included:
   a. nature of the matter
   b. how management intends to respond if the claim is asserted
   c. possible exposure if the claim is asserted
5. Obtain from management a listing of attorneys and legal firms to whom litigation and related matters have been referred. Also, obtain a listing of any litigation noted in the newest review done by internal or external auditors from the examiner assigned internal control, and determine that corrections have been accomplished.
6. Review bills supporting major charges to the general ledger expenses account(s) for legal services as a test of the completeness of the list supplied by the bank.
7. Request that management incorporate information obtained in above steps in a letter to the bank's legal counsel for corroboration.
8. Evaluate management's listing of litigation, unasserted claims and assessments, and counsel's replies for the effect on the financial condition of the bank, giving appropriate consideration to any insurance coverage.
9. Obtain and review copies of any subsequent interim financial statements. Examples of such statements are—
   a. published reports sent to shareholders or others;
   b. reports submitted to the board of directors by internal auditors, external auditors, or management;
   c. statements of condition; and
   d. income statements.
   - Inquire as to whether interim statements obtained were prepared on the same basis as that used for the statements as of the examination date. If not, request proper adjustments to the interim statements.
   - Compare the interim financial statements, especially income statements, with similar statements for the corresponding period in the prior year and to budgets, profit plans, etc., for the current period, if such are available.
   - Obtain from management satisfactory explanations for any unusual items or significant fluctuations noted.
10. Make inquiries of and hold discussions with officers and other executives who have responsibility for the following matters:
    a. changes in credit lines or transactions with officers, directors, controlling shareholders, affiliated bank holding companies, affiliates of an affiliated holding company, or their interests
    b. changes in significant accounting policies
    c. changes in senior officers
    d. any event or combination of events which

have had or could have a material adverse effect on the bank's financial condition, including liquidity, or results of operation, such as the default of a bond issue in which the bank has substantial holdings or the filing of bankruptcy by a major borrower

e. commencement or discontinuance of services not requiring prior approval
f. execution of significant contracts, such as for employment, leases, pension, or other fringe benefit programs
g. significant new contingent liabilities or commitments other than those referred to above
h. significant changes in assets which may not be evident from the review of subsequent interim financial statements, such as a shift in the amount of loans or investments in special categories, or unusual adjustments made in or after the subsequent interim financial statements reviewed in connection with the previous procedure

11. Distribute information obtained in the previous steps to the appropriate examiners. Notify the enforcement section of Board Legal of any investigations or other legal actions being conducted by governmental regulators or criminal prosecutors against the bank when such information is ascertained during the examination process
12. Make additional inquiries or perform such procedures as considered necessary and appropriate to dispose of questions that arose in the course of the preceding procedures, inquiries, and discussions.
13. If, as a result of performing the above procedures, information is obtained that has a significant impact on the evaluation of the soundness of the bank, extend the appropriate examination procedures so that sufficient evidence is reviewed and documented in the workpapers to support the conclusions reached.
14. Prepare comments for the examination report on any events or transaction noted which may have a material effect on the soundness of the bank.
15. Update the workpapers with any information that will facilitate future examinations.

This section sets forth the principal aspects of effective internal control and audit and discusses some pertinent points relative to the internal control questionnaires (ICQs). It assists the examiner in understanding and evaluating the objectives of and the work performed by internal and external auditors. It also sets forth the general criteria the examiner should consider to determine if the work of internal and external auditors can be relied on in the performance of the examination. To the extent that audit records can be relied on, they should be used to complete the ICQs implemented during the examination. In most cases, only those questions not fully supported by audit records would require the examiner to perform a detailed review of the area in question.

Effective internal control is a foundation for the safe and sound operation of a financial institution. The board of directors and senior managers of an institution are responsible for ensuring that the system of internal control is effective. Their responsibility *cannot* be delegated to others within or outside the organization. An internal audit function is an important element of an effective system of internal control. When properly structured and conducted, internal audit provides directors and senior management with vital information about the condition of the system of internal control, and it identifies weaknesses so that management can take prompt, remedial action. Examiners are to review an institution's internal audit function and recommend improvements if needed. In addition, under the Interagency Guidelines Establishing Standards for Safety and Soundness,[1] pursuant to section 39 of the Federal Deposit Insurance Act (FDI Act) (12 USC 1831p-1), each institution is required to have an internal audit function that is appropriate to its size and the nature and scope of its activities.

In summary, internal control is a process designed to provide reasonable assurance that the institution will achieve the following objectives: efficient and effective operations, including safeguarding of assets; reliable financial reporting; and compliance with applicable laws and regulations. Internal control consists of five components that are a part of the management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. The effective functioning of these components, which is brought about by an institution's board of directors, management, and other personnel, is essential to achieving the internal control objectives. This description of internal control is consistent with the Committee of Sponsoring Organizations of the Treadway Commission (COSO) report *Internal Control—Integrated Framework.* In addition, under the COSO framework, financial reporting is defined in terms of published financial statements, which, for these purposes, encompass financial statements prepared in accordance with generally accepted accounting principles and regulatory reports (such as the Reports of Condition and Income). Institutions are encouraged to evaluate their internal control against the COSO framework.

This section includes the March 17, 2003, "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing." In addition, that policy statement is immediately followed by a January 23, 2013, "Federal Reserve Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing," which supplements the 2003 guidance.

AUDIT COMMITTEE OVERSIGHT

Internal and external auditors will not feel free to assess the bank's operations if their independence is compromised. This can sometimes happen when internal and external auditors report solely to senior management instead of to the board of directors.

The independence of internal and external auditors is increased when they report to an independent audit committee (one made up of external directors who are not members of the bank's management). The auditors' independence is enhanced when the audit committee takes an active role in approving the internal and external audit scope and plan.

The role of the independent audit committee is important. The audit committee's duties may include (1) overseeing the internal audit function; (2) approving or recommending the appointment of external auditors and the scope

1. For state member banks, see appendix D-1 to 12 CFR 208.

of external audits and other services; (3) providing the opportunity for auditors to meet and discuss findings apart from management; (4) reviewing with management and external auditors the year-end financial statements; and (5) meeting with regulatory authorities.

Public Company Accounting Oversight Board

The Sarbanes-Oxley Act of 2002 (the act) became law on July 30, 2002 (Pub. L. No. 107-204). The act addresses weaknesses in corporate governance and the accounting and auditing professions and includes provisions addressing audits, financial reporting and disclosure, conflicts of interest, and corporate governance at publicly owned companies. The act, among other things, requires public companies to have an audit committee made entirely of independent directors. Publicly owned banking organizations that are listed on the New York Stock Exchange (NYSE) and Nasdaq must also comply with those exchanges' listing requirements, which include audit committee requirements.

The act also established a Public Company Accounting Oversight Board (PCAOB) that has the authority to set and enforce auditing, attestation, quality-control, and ethics (including independence) standards for auditors of public companies (subject to Securities and Exchange Commission (SEC) review). (See SR-02-20.) Accounting firms that conduct audits of public companies (registered accounting firms) must register with the PCAOB and be subject to its supervision. The PCAOB is also empowered to inspect the auditing operations of public accounting firms that audit public companies as well as impose disciplinary and remedial sanctions for violations of its rules, securities laws, and professional auditing and accounting standards. (See www.pcaobus.org.)

Nonpublic banking organizations are encouraged to periodically review their policies and procedures relating to corporate-governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the organization's size, operations, and resources. Furthermore, a banking organization's policies and procedures for corporate governance, internal controls, and auditing will be assessed during the supervisory process, and supervisory action may be taken if there are deficiencies or weaknesses in these areas that are inconsistent with sound corporate-governance practices or safety-and-soundness considerations.

DISCIPLINARY ACTIONS AGAINST ACCOUNTANTS AND ACCOUNTING FIRMS PERFORMING CERTAIN AUDIT SERVICES

Section 36 of the Federal Deposit Insurance Act (the FDI Act) authorizes the federal bank and thrift regulatory agencies (the agencies)[2] to take disciplinary actions against independent public accountants and accounting firms that perform audit services covered by the act's provisions. Section 36, as implemented by part 363 of the FDIC's rules (12 CFR 363), requires that each federally insured depository institution with total assets of $500 million or more obtain an audit of its financial statements and a management report. Institutions with assets of $1 billion or more must provide an attestation on management's assertions concerning internal controls over financial reporting that is performed by an independent public accountant (the accountant). The respective insured depository institution must include the accountant's audit and attestation reports in its annual report, as required. See the section on "Legal Requirements Affecting Banks and the Audit Function."

The agencies amended their rules, pursuant to section 36, that set forth the practices and procedures to implement their authority to remove, suspend, or debar, for good cause,[3] an accountant or firm from performing audit and attestation services for insured depository institutions with assets of $500 million or more.[4] Immediate suspensions are permitted in limited circum-

2. The Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation. The Board approved its rules on August 6, 2003 (press release of August 8, 2003). The rules became effective October 1, 2003. They were later revised as of July 20, 2009.

3. The rules provide that certain violations of law, negligent conduct, reckless violations of professional standards, or lack of qualifications to perform auditing services may be considered good cause.

4. See the Federal Reserve's rules on disciplinary actions against public accountants and accounting firms at 12 CFR 263.94 and 12 CFR 263, subpart J.

stances. Also, an accountant or accounting firm is prohibited from performing audit services for the covered institution if an authorized agency has taken such a disciplinary action against the accountant or firm, or if the SEC or the PCAOB has taken certain disciplinary action against the accountant or firm.

The amended rules reflect the agencies' increasing concern about the quality of audits and internal controls for financial reporting at insured depository institutions. The rules emphasize the importance of maintaining high quality in the audits of federally insured depository institutions' financial position and in the attestations of management assessments.

OBJECTIVES OF INTERNAL CONTROL

In general, good internal control exists when no one is in a position to make significant errors or perpetrate significant irregularities without timely detection. Therefore, a system of internal control should include those procedures necessary to ensure timely detection of failure of accountability, and such procedures should be performed by competent persons who have no incompatible duties. The following standards are encompassed within the description of internal control:

Existence of procedures. Existence of prescribed internal control procedures is necessary but not sufficient for effective internal control. Prescribed procedures that are not actually performed do nothing to establish control. Consequently, the examiner must give thoughtful attention not only to the prescribed set of procedures but also to the practices actually followed. This attention can be accomplished through inquiry, observation, testing, or a combination thereof.

Competent performance. For internal control to be effective, the required procedures must be performed by competent persons. Evaluation of competence undoubtedly requires some degree of subjective judgment because attributes such as intelligence, knowledge, and attitude are relevant. Thus, the examiner should be alert for indications that employees have failed so substantially to perform their duties that a serious question is raised concerning their abilities.

Independent performance. If employees who have access to assets also have access to the related accounting records or perform related review operations (or immediately supervise the activities of other employees who maintain the records or perform the review operations), they may be able to both perpetrate and conceal defalcations. Therefore, duties concerned with the custody of assets are incompatible with recordkeeping duties for those assets, and duties concerned with the performance of activities are incompatible with the authorization or review of those activities.

In judging the independence of a person, the examiner must avoid looking at that person as an individual and presuming the way in which that individual would respond in a given situation. For example, an individual may be the sole check signer and an assistant may prepare monthly bank reconcilement. If the assistant appears to be a competent person, it may seem that an independent reconcilement would be performed and anything amiss would be reported. Such judgments are potentially erroneous. There exist no established tests by which the psychological and economic independence of an individual in a given situation can be judged. The position must be evaluated, not the person. If the position in which the person acts is not an independent one in itself, then the work should not be presumed to be independent, regardless of the apparent competence of the person in question. In the example cited above, the function performed by the assistant should be viewed as if it were performed by the supervisor. Hence, incompatible duties are present in that situation.

PROCEDURES FOR COMPLETING ICQs

The implementation of selected ICQs and the evaluation of internal audit activities provide a basis for determining the adequacy of the bank's control environment. To reach conclusions required by the questionnaires, the examiner assigned to review a given internal control routine or area of bank operations should use any source of information necessary to ensure a full understanding of the prescribed system, including any potential weaknesses. Only when the examiner completely understands the bank's system can an assessment and evaluation be

made of the effects of internal controls on the examination.

To reach conclusions concerning a specific section of an ICQ, the examiner should document and review the bank's operating systems and procedures by consulting all available sources of information and discussing them with appropriate bank personnel. Sources of information might include organization charts, procedural manuals, operating instructions, job specifications, directives to employees, and other similar sources of information. Also, the examiner should not overlook potential sources such as job descriptions, flow charts, and other documentation in the internal audit workpapers. A primary objective in the review of the system is to efficiently reach a conclusion about the overall adequacy of existing controls. Any existing source of information that will enable the examiner to quickly gain an understanding of the procedures in effect should be used in order to minimize the time required to formulate the conclusions. The review should be documented in an organized manner through the use of narrative descriptions, flow charts, or other diagrams. If a system is properly documented, the documentation will provide a ready reference for any examiner performing work in the area, and it often may be carried forward for future examinations, which will save time.

Although narrative descriptions can often provide an adequate explanation of systems of internal control, especially in less complex situations, they may have certain drawbacks, such as the following:

- They may be cumbersome and too lengthy.
- They may be unclear or poorly written.
- Related points may be difficult to integrate.
- Annual changes may be awkward to record.

To overcome these problems, the examiner should consider using flow charts, which reduce narrative descriptions to a picture. Flow charts often reduce a complex situation to an easily understandable sequence of interrelated steps.

In obtaining and substantiating the answers to the questions in the ICQ, the examiner should develop a plan to obtain the necessary information efficiently. Such a plan would normally avoid a direct question-and-answer session with bank officers. A suggested approach to completion of the ICQ is to—

- become familiar with the ICQ,
- review related internal audit procedures, reports, and responses,
- review any written documentation of a bank's system of controls,
- find out what the department does and what the functions of personnel within the department are through conversations with appropriate individuals, and
- answer as many individual questions as possible from information gained in the preceding steps and fill in the remaining questions by direct inquiry.

An effective way to begin an on-site review of internal control is to identify the various key functions applicable to the area under review. For each position identified, the following questions should then be asked:

- Is this a critical position? That is, can a person in this position either make a significant error that will affect the recording of transactions or perpetrate material irregularities of some type?
- If an error is made or an irregularity is perpetrated, what is the probability that normal routines will disclose it on a timely basis? That is, what controls exist that would prevent or detect significant errors or the perpetration of significant irregularities?
- What are the specific opportunities open to the individual to conceal any irregularity, and are there any mitigating controls that will reduce or eliminate these opportunities?

Although all employees within an organization may be subject to control, not all have financial responsibilities that can influence the accuracy of the accounting and financial records or have access to assets. The examiner should be primarily concerned with those positions that have the ability to influence the records and that have access to assets. Once those positions have been identified, the examiners must exercise their professional knowledge of bank operations to visualize the possibilities open to any person holding a particular position. The question is not whether the individual is honest, but rather whether situations exist that might permit an error to be concealed. By directing attention to such situations, an examiner will also consider situations that may permit unintentional errors to remain undetected.

The evaluation of internal control should include consideration of other existing accounting and administrative controls or other circum-

stances that might counteract or mitigate an apparent weakness or impair an established control. Controls that mitigate an apparent weakness may be a formal part of the bank's operating system, such as budget procedures that include a careful comparison of budgeted and actual amounts by competent management personnel. Mitigating controls also may be informal. For example, in small banks, management may be sufficiently involved in daily operations to know the purpose and reasonableness of all expense disbursements. That knowledge, coupled with the responsibility for signing checks, may make irregularities by nonmanagement personnel unlikely, even if disbursements are otherwise under the control of only one person.

When reviewing internal controls, an essential part of the examination is being alert to indications that adverse circumstances may exist. Adverse circumstances may lead employees or officers into courses of action they normally would not pursue. An adverse circumstance to which the examiner should be especially alert exists when the personal financial interests of key officers or employees depend directly on operating results or financial condition. Although the review of internal control does not place the examiner in the role of an investigator or detective, an alert attitude toward possible conflicts of interest should be maintained throughout the examination. Also, offices staffed by members of the same family, branches completely dominated by a strong personality, or departments in which supervisors rely unduly on their assis-tants require special alertness on the part of the examiner. Those circumstances and other similar ones should be considered in preparing the ICQ. It is not the formality of the particular factor that is of importance but rather its effect on the overall operation under review. Circumstances that may affect answers to the basic questions should be noted along with conclusions concerning their effect on the examination.

The ICQs were designed so that answers could be substantiated by (1) inquiry to bank personnel, (2) observation, or (3) testing. However, certain questions are marked with an asterisk to indicate that they require substantiation through observation or testing. Those questions are deemed so critical that substantiation by inquiry is not sufficient. For those questions substantiated through testing, the nature and extent of the test performed should be indicated adjacent to the applicable step in the ICQ.

The examiner should be alert for deviations by bank personnel from established policies, practices, and procedures. This applies not only to questions marked with an asterisk but also to every question in the ICQ. Examples of such deviations include situations when (1) instructions and directives are frequently not revised to reflect current practices, (2) employees find shortcuts for performing their tasks, (3) changes in organization and activities may influence operating procedures in unexpected ways, or (4) employees' duties may be rotated in ways that have not been previously considered. These and other circumstances may serve to modify or otherwise change prescribed procedures, thus giving the examiner an inadequate basis for evaluating internal control.

Sometimes, when a substantial portion of the accounting work is accomplished by computer, the procedures are so different from conventional accounting methods that the principles discussed here seem inapplicable. Care should be taken to resist drawing this conclusion. This discussion of internal control and its evaluation is purposely stated in terms sufficiently general to apply to any system. Perpetration of defalcations requires direct or indirect access to appropriate documents or accounting records. As such, perpetration requires the involvement of people and, under any system, computerized or not, there will be persons who have access to assets and records. Those with access may include computer operators, programmers, and their supervisors and other related personnel.

The final question in each section of the ICQ requires a composite evaluation of existing internal controls in the applicable area of the bank. The examiner should base that evaluation on answers to the preceding questions within the section, the review and observation of the systems and controls within the bank, and discussion with appropriate bank personnel.

The composite evaluation does, however, require some degree of subjective judgment. The examiner should use all information available to formulate an overall evaluation, fully realizing that a high degree of professional judgment is required.

Applying the ICQ to Different Situations

The ICQs are general enough to apply to a wide range of systems, so not all sections or questions will apply to every situation, depending on factors such as bank size, complexity and type of operations, and organizational structure. When completing the ICQs, the examiner should include a brief comment stating the reason a section or question is not applicable to the specific situation.

For large banking institutions or when multiple locations of a bank are being examined, it may be necessary to design supplements to the ICQs to adequately review all phases of the bank's operations and related internal controls. Because certain functions described in this manual may be performed by several departments in some banks, it also may be necessary to redesign a particular section of the ICQ so that each department receives appropriate consideration. Conversely, functions described in several different sections of this handbook may be performed in a single department in smaller banks. If the ICQ is adapted to fit a specific situation, care should be taken to ensure that its scope and intent are not modified. That requires professional judgment in interpreting and expanding the generalized material. Any such modifications should be completely documented and filed in the workpapers.

LEGAL REQUIREMENTS AFFECTING BANKS AND THE AUDIT FUNCTION

The Federal Deposit Insurance Corporation Improvement Act of 1991 amended section 36 of the FDI Act (12 USC 1831m). Since then, the FDIC has made various revisions to its rules at Part 363 (12 CFR 363) and guidelines. When specific reports are required to be submitted to the FDIC to comply with the provisions of compliance with Part 363, the institution must also submit the report to the appropriate federal banking agency and any appropriate state supervisor.

For the purposes of determining the applicability of this rule, an institution should use total assets as reported on its most recent Report of Condition (the Call Report), the date that coincides with the end of the preceding fiscal year. If the fiscal year ends on a date other than the end of a calendar quarter, the institution is to use the Call Report for the quarter end immediately preceding the end of the fiscal year.

Institutions with $500 Million or More in Total Assets

The regulations require these institutions to file two copies of their annual reports with the FDIC, as well as with the appropriate federal banking agency and the appropriate state supervisory agency, that must include the following:

- Audited comparative annual financial statements;
- The independent public accountant's report on the audited financial statements;
- A management report (comprising its statements and assessments) that is signed by the chief executive officer and chief accounting or chief financial officer. The report should include:
  - — A statement of management's responsibilities for:
    - preparing the annual financial statements;
    - establishing and maintaining an adequate internal control structure and procedures over financial reporting;
    - complying with designated safety-and-soundness laws and regulations pertaining to insider loans and dividend restrictions; and
  - — An assessment by management of:
    - compliance with the designated safety-and-soundness laws and regulations pertaining to insider loans and dividend restrictions during the year, which must state management's conclusions regarding compliance and disclose any noncompliance with these laws and regulations.[5] (See SR-13-11.)

If the institution is a public company or a subsidiary of a public company that would be subject to the provisions of section 404 of the Sarbanes-Oxley Act (Section 404), it must comply with the requirement to file other reports issued by the independent accountant as set forth in section 363.4(c) (12 CFR 363.4(c)). The

5. See appendix B of 12 CFR part 363 for further details and illustrative examples of the appropriate wording for the management report.

institutions must provide a copy of the independent accountant's report to the FDIC on the audit of internal control over financial reporting that is required by section 404 with the FDIC within 15 days after receipt. The institutions also are encouraged to submit a copy of management's section 404 report on internal control over financial reporting together with the independent public accountant's internal control report.

Institutions with $1 Billion or More in Total Assets

Section 36 of the FDI Act and Part 363 of the FDIC's regulations required insured depository institutions with a least $1 billion in total assets to file two copies of additional reports that must include the following:

- Assessments by management of the effectiveness of the institution's internal control structure and procedures over financial reporting as of the end of the fiscal year (12 USC 1831m(b)(2)(B)(i); and
- The independent public accountant's attestation report—the independent public accountant is to examine, attest to, and report separately in an attestation report, on the assertions by management's concerning the institution's internal control structure and procedures for financial reporting (12 USC 1831m(c)). This includes the Call Report and the FR Y-9C report. The attestation is to be made in accordance with generally accepted standards for attestation engagements.

Other Requirements—Institutions with $500 Million or More in Total Assets

Financial reporting encompasses, for the purposes of Part 363, both financial statements prepared in accordance with generally accepted accounting principles and those prepared for regulatory reporting purposes. Each institution is to have an independent public accountant perform an audit who reports on the institution's annual financial statements in accordance with generally accepted auditing standards and section 37 of the FDI Act (12 USC 1831n). The scope of the audit engagement must be sufficient to permit the accountant to determine and report whether the financial statements are presented fairly and in accordance with generally accepted accounting principles. The audit is to be performed using procedures that will objectively determine the accuracy of management's assertions on compliance with safety-and-soundness laws and regulations (12 USC 1831m (b)(2)(A)(iii)).

In addition, each institution is required to file a copy of any management letter, qualification, or any other report issued by its independent public accountant with the FDIC within 15 days of receipt of such letter or report. See section 363.4(c) (12 CFR 363.4(c)).

Each institution is required to establish an audit committee of its board of directors. The duties of the audit committee include reviewing with management and the independent public accountant the basis for, and the results of, the annual independent audit reports and the institution's respective reporting requirements. Each institution with total assets of $1 billion or more, as of the beginning of the fiscal year, is required to have an audit committee, the members of which must be outside directors who are independent of the institution's management. Institutions with total assets of $500 million, but less than $1 billion or more, as of the beginning of the fiscal year, must have an audit committee, the members of which are outside directors, the majority of whom must be independent of the institution's management.

Reporting Requirements for Subsidiaries of Holding Companies

Under the FDIC rules, an insured depository institution that is a subsidiary of a holding company may file its audited financial statements at the holding company level (top-tier or mid-tier) if the holding company has total insured depository institution assets comprising 75 percent or more of the holding company's consolidated assets as of the beginning of the fiscal year. Furthermore, in accordance with 12 CFR part 363, the other reporting requirements can be satisfied at the holding company level if the holding company provides services and functions comparable to the insured depository institution, and the insured depository subsidiary (a) has less than $5 billion in total assets or (b) has a CAMELS composite rating of "1" or "2" when its total assets are $5 billion or more.

In order to facilitate effective and prudential supervision of the holding company, a holding

company that has institutions subject to the FDIC rules must submit one copy of the required reports to the appropriate Federal Reserve Bank regardless of whether or not the holding company submitted these reports on a consolidated basis for its insured depository subsidiaries, and regardless of the charter of the insured depository subsidiary under the holding company. Refer to SR letter 94-3, "Supervisory Guidance on the Implementation of Section 112 of the FDIC Improvement Act," for further guidance on this filing requirement. (See SR-13-11.)

Required Management Report Signatures

As specified in 12 CFR part 363, an insured depository institution and holding company must adhere to the following signature requirements:

- If the audited financial statements and the management report requirements are satisfied entirely at the insured depository institution level, the management report must be signed by the CEO, as well as the CAO or CFO, at the insured depository institution level.
- If the audited financial statements and the management report requirements are satisfied entirely at the holding company level, the management report must be signed by the CEO, as well as the CAO or CFO, at the holding company level.
- If the audited financial statement requirements are satisfied at the holding company level and the management report requirement is satisfied at the insured depository institution level or one or more component requirements are satisfied at the holding company and the remaining component requirements are satisfied at the insured depository institution level, the management report must be signed by the CEO, as well as the CAO or CFO, of both the holding company and the insured depository institution.

INTERAGENCY POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING

The Federal Reserve and other federal banking agencies[6] (the agencies) adopted on March 17, 2003, an interagency policy statement addressing the internal audit function and its outsourcing. The policy statement revises and replaces the former 1997 policy statement and incorporates recent developments in internal auditing. In addition, the revised policy incorporates guidance on the independence of accountants who provide institutions with both internal and external audit services in light of the Sarbanes-Oxley Act of 2002 (the act) and associated SEC rules.

The act prohibits an accounting firm from acting as the external auditor of a public company during the same period that the firm provides internal audit services to the company. The policy statement discusses the applicability of this prohibition to institutions that are public companies, to insured depository institutions with assets of $500 million or more that are subject to the annual audit and reporting requirements of section 36 of the FDI Act, and to nonpublic institutions that are not subject to section 36.

The statement recognizes that many institutions have engaged independent public accounting firms and other outside professionals (outsourcing vendors) to perform work that traditionally has been done by internal auditors. These arrangements are often called "internal audit outsourcing," "internal audit assistance," "audit co-sourcing," and "extended audit services" (hereafter collectively referred to as outsourcing). Typical outsourcing arrangements are more fully described below.

Outsourcing may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. However, the structure, scope, and management of some internal audit outsourcing arrangements may not contribute to the institution's safety and soundness. Furthermore, arrangements with outsourcing vendors should not leave directors and senior management with the erroneous impression that they have been relieved of their responsibility for maintaining an effective system of internal control and for overseeing the internal audit function.

6. The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency.

Internal Audit Function (Part I)

Board and Senior Management Responsibilities

The board of directors and senior management are responsible for having an effective system of internal control and an effective internal audit function in place at their institution. They are also responsible for ensuring that the importance of internal control is understood and respected throughout the institution. This overall responsibility cannot be delegated to anyone else. They may, however, delegate the design, implementation, and monitoring of specific internal controls to lower-level management and delegate the testing and assessment of internal controls to others. Accordingly, directors and senior management should have reasonable assurance that the system of internal control prevents or detects significant inaccurate, incomplete, or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial reporting (which includes regulatory reporting); and deviations from laws, regulations, and the institution's policies.[7]

Some institutions have chosen to rely on so-called management self-assessments or control self-assessments, wherein business-line managers and their staff evaluate the performance of internal controls within their purview. Such reviews help to underscore management's responsibility for internal control, but they are not impartial. Directors and members of senior management who rely too much on these reviews may not learn of control weaknesses until they have become costly problems, particularly if directors are not intimately familiar with the institution's operations. Therefore, institutions generally should also have their internal controls tested and evaluated by units without business-line responsibilities, such as internal audit groups.

Directors should be confident that the internal audit function addresses the risks of and meets the demands posed by the institution's current and planned activities. To accomplish this objective, directors should consider whether their institution's internal audit activities are conducted in accordance with professional standards, such as the Institute of Internal Auditors' (IIA) *Standards for the Professional Practice of Internal Auditing.* These standards address independence, professional proficiency, scope of work, performance of audit work, management of internal audit, and quality-assurance reviews. Furthermore, directors and senior management should ensure that the following matters are reflected in their institution's internal audit function.

Structure. Careful thought should be given to the placement of the audit function in the institution's management structure. The internal audit function should be positioned so that the board has confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations. The audit committee,[8] using objective criteria it has established, should oversee the internal audit function and evaluate its performance.[9] The audit committee should assign responsibility for the internal audit function to a member of management (that is, the manager of internal audit or internal audit manager) who understands the function and has no responsibility for operating the system of internal control. The ideal organizational arrange-

7. As noted above, under section 36 of the FDI Act, as implemented by part 363 of the FDIC's regulations (12 CFR 363), FDIC-insured depository institutions with total assets of $500 million or more must submit an annual management report signed by the chief executive officer (CEO) and chief accounting or chief financial officer. This report must contain (1) a statement of management's responsibilities for preparing the institution's annual financial statements, for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and for complying with designated laws and regulations relating to safety and soundness, including management's assessment of the institution's compliance with those laws and regulations, and (2) for an institution with total assets of $1 billion or more at the beginning of the institution's most recent fiscal year, an assessment by management of the effectiveness of such internal control structure and procedures as of the end of such fiscal year. (See 12 CFR 363.2(b) and 70 *Fed. Reg.* 71,232, Nov. 28, 2005.)

8. Depository institutions subject to section 36 of the FDI Act and part 363 of the FDIC's regulations must maintain independent audit committees (i.e., consisting of directors who are not members of management). Consistent with the 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations, the agencies also encourage the board of directors of each depository institution that is not otherwise required to do so to establish an audit committee consisting entirely of outside directors. Where the term *audit committee* is used in this policy statement, the board of directors may fulfill the audit committee responsibilities if the institution is not subject to an audit committee requirement. See *Fed. Reg.,* September 28, 1999 (64 FR 52,319).

9. For example, the performance criteria could include the timeliness of each completed audit, a comparison of overall performance to plan, and other measures.

ment is for this manager to report directly and solely to the audit committee regarding both audit issues and administrative matters, for example, resources, budget, appraisals, and compensation. Institutions are encouraged to consider the IIA's *Practice Advisory 2060-2: Relationship with the Audit Committee,* which provides more guidance on the roles and relationships between the audit committee and the internal audit manager.

Many institutions place the manager of internal audit under a dual reporting arrangement: the manager is functionally accountable to the audit committee on issues discovered by the internal audit function, while reporting to another senior manager on administrative matters. Under a dual reporting relationship, the board should consider the potential for diminished objectivity on the part of the internal audit manager with respect to audits concerning the executive to whom he or she reports. For example, a manager of internal audit who reports to the chief financial officer (CFO) for performance appraisal, salary, and approval of department budgets may approach audits of the accounting and treasury operations controlled by the CFO with less objectivity than if the manager were to report to the chief executive officer. Thus, the chief financial officer, controller, or other similar officer should ideally be excluded from overseeing the internal audit activities even in a dual role. The objectivity and organizational stature of the internal audit function are best served under such a dual arrangement if the internal audit manager reports administratively to the CEO.

Some institutions seek to coordinate the internal audit function with several risk-monitoring functions (for example, loan-review, market-risk-assessment, and legal compliance departments) by establishing an administrative arrangement under one senior executive. Coordination of these other monitoring activities with the internal audit function can facilitate the reporting of material risk and control issues to the audit committee, increase the overall effectiveness of these monitoring functions, better utilize available resources, and enhance the institution's ability to comprehensively manage risk. Such an administrative reporting relationship should be designed so as to not interfere with or hinder the manager of internal audit's functional reporting to and ability to directly communicate with the institution's audit committee. In addition, the audit committee should ensure that efforts to coordinate these monitoring functions do not result in the manager of internal audit conducting control activities nor diminish his or her independence with respect to the other risk-monitoring functions. Furthermore, the internal audit manager should have the ability to independently audit these other monitoring functions.

In structuring the reporting hierarchy, the board should weigh the risk of diminished independence against the benefit of reduced administrative burden in adopting a dual reporting organizational structure. The audit committee should document its consideration of this risk and mitigating controls. The IIA's *Practice Advisory 1110-2: Chief Audit Executive Reporting Lines* provides additional guidance regarding functional and administrative reporting lines.

Management, staffing, and audit quality. In managing the internal audit function, the manager of internal audit is responsible for control risk assessments, audit plans, audit programs, and audit reports.

- A control risk assessment (or risk-assessment methodology) documents the internal auditor's understanding of the institution's significant business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line, the mitigating control processes, and the resulting residual risk exposure of the institution. They should be updated regularly to reflect changes to the system of internal control or work processes and to incorporate new lines of business.
- An internal audit plan is based on the control risk assessment and typically includes a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.
- An internal audit program describes the objectives of the audit work and lists the procedures that will be performed during each internal audit review.
- An audit report generally presents the purpose, scope, and results of the audit, including findings, conclusions, and recommendations. Workpapers that document the work performed and support the audit report should be maintained.

Ideally, the internal audit function's only role should be to independently and objectively

evaluate and report on the effectiveness of an institution's risk-management, control, and governance processes. Internal auditors increasingly have taken a consulting role within institutions on new products and services and on mergers, acquisitions, and other corporate reorganizations. This role typically includes helping design controls and participating in the implementation of changes to the institution's control activities. The audit committee, in its oversight of the internal audit staff, should ensure that the function's consulting activities do not interfere or conflict with the objectivity it should have with respect to monitoring the institution's system of internal control. In order to maintain its independence, the internal audit function should not assume a business-line management role over control activities, such as approving or implementing operating policies or procedures, including those it has helped design in connection with its consulting activities. The agencies encourage internal auditors to follow the IIA's standards, including guidance related to the internal audit function acting in an advisory capacity.

The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and assess whether internal controls are effective. The manager of internal audit should oversee the staff assigned to perform the internal audit work and should establish policies and procedures to guide the audit staff. The form and content of these policies and procedures should be consistent with the size and complexity of the department and the institution. Many policies and procedures may be communicated informally in small internal audit departments, while larger departments would normally require more formal and comprehensive written guidance.

Scope. The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's on- and off-balance-sheet activities. At least annually, the audit committee should review and approve internal audit's control risk assessment and the scope of the audit plan, including how much the manager relies on the work of an outsourcing vendor. It should also periodically review internal audit's adherence to the audit plan. The audit committee should consider requests for expansion of basic internal audit work when significant issues arise or when significant changes occur in the institution's environment, structure, activities, risk exposures, or systems.[10]

Communication. To properly carry out their responsibility for internal control, directors and senior management should foster forthright communications and critical examination of issues to better understand the importance and severity of internal control weaknesses identified by the internal auditor and operating management's solutions to these weaknesses. Internal auditors should report internal control deficiencies to the appropriate level of management as soon as they are identified. Significant matters should be promptly reported directly to the board of directors (or its audit committee) and senior management. In periodic meetings with management and the manager of internal audit, the audit committee should assess whether management is expeditiously resolving internal control weaknesses and other exceptions. Moreover, the audit committee should give the manager of internal audit the opportunity to discuss his or her findings without management being present.

Furthermore, each audit committee should establish and maintain procedures for employees of their institution to confidentially and anonymously submit concerns to the committee about questionable accounting, internal accounting control, or auditing matters.[11] In addition, the audit committee should set up procedures for the timely investigation of complaints received and the retention for a reasonable time period of documentation concerning the complaint and its subsequent resolution.

Contingency planning. As with any other function, the institution should have a contingency plan to mitigate any significant discontinuity in audit coverage, particularly for high-risk areas. Lack of contingency planning for continuing internal audit coverage may increase the institution's level of operational risk.

10. Major changes in an institution's environment and conditions may compel changes to the internal control system and also warrant additional internal audit work. These changes include (1) new management; (2) areas or activities experiencing rapid growth or rapid decline; (3) new lines of business, products, or technologies or disposals thereof; (4) corporate restructurings, mergers, and acquisitions; and (5) an expansion or acquisition of foreign operations (including the impact of changes in the related economic and regulatory environments).

11. When the board of directors fulfills the audit committee responsibilities, the procedures should provide for the submission of employee concerns to an outside director.

Small Financial Institution's Internal Audit Function

An effective system of internal control and an independent internal audit function form the foundation for safe and sound operations, regardless of an institution's size. Each institution should have an internal audit function that is appropriate to its size and the nature and scope of its activities. The procedures assigned to this function should include adequate testing and review of internal controls and information systems.

It is the responsibility of the audit committee and management to carefully consider the extent of auditing that will effectively monitor the internal control system, after taking into account the internal audit function's costs and benefits. For institutions that are large or have complex operations, the benefits derived from a full-time manager of internal audit or an auditing staff likely outweigh the cost. For small institutions with few employees and less complex operations, however, these costs may outweigh the benefits. Nevertheless, a small institution without an internal auditor can ensure that it maintains an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls. The key characteristic of such reviews is that the persons directing and/or performing the review of internal controls are *not* also responsible for managing or operating those controls. A person who is competent in evaluating a system of internal control should design the review procedures and arrange for their implementation. The person responsible for reviewing the system of internal control should report findings directly to the audit committee. The audit committee should evaluate the findings and ensure that senior management has or will take appropriate action to correct the control deficiencies.

Internal Audit Outsourcing Arrangements (Part II)

Examples of Internal Audit Outsourcing Arrangements

An outsourcing arrangement is a contract between an institution and an outsourcing vendor to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. Some institutions consider entering into these arrangements to enhance the quality of their control environment by obtaining the services of a vendor with the knowledge and skills to critically assess, and recommend improvements to, their internal control systems. The internal audit services under contract can be limited to helping internal audit staff in an assignment for which they lack expertise. Such an arrangement is typically under the control of the institution's manager of internal audit, and the outsourcing vendor reports to him or her. Institutions often use outsourcing vendors for audits of areas requiring more technical expertise, such as electronic data processing and capital-markets activities. Such uses are often referred to as "internal audit assistance" or "audit co-sourcing."

Some outsourcing arrangements may require an outsourcing vendor to perform virtually all the procedures or tests of the system of internal control. Under such an arrangement, a designated manager of internal audit oversees the activities of the outsourcing vendor and typically is supported by internal audit staff. The outsourcing vendor may assist the audit staff in determining risks to be reviewed and may recommend testing procedures, but the internal audit manager is responsible for approving the audit scope, plan, and procedures to be performed. Furthermore, the internal audit manager is responsible for the results of the outsourced audit work, including findings, conclusions, and recommendations. The outsourcing vendor may report these results jointly with the internal audit manager to the audit committee.

Additional Considerations for Internal Audit Outsourcing Arrangements

Even when outsourcing vendors provide internal audit services, the board of directors and senior management of an institution are responsible for ensuring that both the system of internal control and the internal audit function operate effectively. In any outsourced internal audit arrangement, the institution's board of directors and senior management must maintain ownership of the internal audit function and provide active oversight of outsourced activities. When negotiating the outsourcing arrangement with an outsourcing vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit

responsibilities. The outsourcing arrangement should not increase the risk that a breakdown of internal control will go undetected.

To clearly distinguish its duties from those of the outsourcing vendor, the institution should have a written contract, often taking the form of an engagement letter.[12] Contracts between the institution and the vendor typically include provisions that—

- define the expectations and responsibilities under the contract for both parties;
- set the scope and frequency of, and the fees to be paid for, the work to be performed by the vendor;
- set the responsibilities for providing and receiving information, such as the type and frequency of reporting to senior management and directors about the status of contract work;
- establish the process for changing the terms of the service contract, especially for expansion of audit work if significant issues are found, and stipulations for default and termination of the contract;
- state that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related workpapers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the workpapers prepared by the outsourcing vendor;
- specify the locations of internal audit reports and the related workpapers;
- specify the period of time (for example, seven years) that vendors must maintain the workpapers;[13]
- state that outsourced internal audit services provided by the vendor are subject to regulatory review and that examiners will be granted full and timely access to the internal audit reports and related workpapers prepared by the outsourcing vendor;
- prescribe a process (arbitration, mediation, or other means) for resolving disputes and for determining who bears the cost of consequential damages arising from errors, omissions, and negligence; and
- state that the outsourcing vendor will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of a member of management or an employee and, if applicable, will comply with AICPA, U.S. Securities and Exchange Commission (SEC), PCAOB, or regulatory independence guidance.

Vendor competence. Before entering an outsourcing arrangement, the institution should perform due diligence to satisfy itself that the outsourcing vendor has sufficient staff qualified to perform the contracted work. The staff's qualifications may be demonstrated, for example, through prior experience with financial institutions. Because the outsourcing arrangement is a personal-services contract, the institution's internal audit manager should have confidence in the competence of the staff assigned by the outsourcing vendor and receive timely notice of key staffing changes. Throughout the outsourcing arrangement, management should ensure that the outsourcing vendor maintains sufficient expertise to effectively perform its contractual obligations.

Management of the outsourced internal audit function. Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ sufficient competent staff members in the internal audit department to assist the manager of internal audit in overseeing the outsourcing vendor. Small institutions that do not employ a full-time audit manager should appoint a competent employee who ideally has no managerial responsibility for the areas being audited to oversee the outsourcing vendor's performance under the contract. This person should report directly to the audit committee for purposes of communicating internal audit issues.

Communication when an outsourced internal audit function exists. Communication between the internal audit function and the audit committee and senior management should not

12. The engagement-letter provisions described are comparable to those outlined by the American Institute of Certified Public Accountants (AICPA) for financial statement audits. (See AICPA Professional Standards, AU section 310.) These provisions are consistent with the provisions customarily included in contracts for other outsourcing arrangements, such as those involving data processing and information technology. Therefore, the federal banking agencies consider these provisions to be usual and customary business practices.

13. If the workpapers are in electronic format, contracts often call for the vendor to maintain proprietary software that enables the bank and examiners to access the electronic workpapers for a specified time period.

diminish because the institution engages an outsourcing vendor. All work by the outsourcing vendor should be well documented and all findings of control weaknesses should be promptly reported to the institution's manager of internal audit. Decisions not to report the outsourcing vendor's findings to directors and senior management should be the mutual decision of the internal audit manager and the outsourcing vendor. In deciding what issues should be brought to the board's attention, the concept of "materiality," as the term is used in financial statement audits, is generally not a good indicator of which control weakness to report. For example, when evaluating an institution's compliance with laws and regulations, any exception may be important.

Contingency planning to ensure continuity of outsourced audit coverage. When an institution enters into an outsourcing arrangement (or significantly changes the mix of internal and external resources used by internal audit), it may increase its operational risk. Because the arrangement may be terminated suddenly, the institution should have a contingency plan to mitigate any significant discontinuity in audit coverage, particularly for high-risk areas.

Independence of the Independent Public Accountant (Part III)

The following discussion applies only when a financial institution is considering using a public accountant to provide both external audit and internal audit services to the institution.

When one accounting firm performs both the external audit and the outsourced internal audit function, the firm risks compromising its independence. These concerns arise because, rather than having two separate functions, this outsourcing arrangement places the independent public accounting firm in the position of appearing to audit, or actually auditing, its own work. For example, in auditing an institution's financial statements, the accounting firm will consider the extent to which it may rely on the internal control system, including the internal audit function, in designing audit procedures.

Applicability of the SEC's Auditor Independence Requirements

Institutions that are public companies. To strengthen auditor independence, Congress passed the Sarbanes-Oxley Act of 2002 (the act). Title II of the act applies to any public company—that is, any company that has a class of securities registered with the SEC or the appropriate federal banking agency under section 12 of the Securities Exchange Act of 1934 or that is required to file reports with the SEC under section 15(d) of that act.[14] The act prohibits an accounting firm from acting as the external auditor of a public company during the same period that the firm provides internal audit outsourcing services to the company.[15] In addition, if a public company's external auditor will be providing auditing services and permissible nonaudit services, such as tax services, the company's audit committee must preapprove each of these services.

According to the SEC's final rules (effective May 6, 2003) implementing the act's nonaudit-service prohibitions and audit committee preapproval requirements, an accountant is not independent if, at any point during the audit and professional engagement period, the accountant provides internal audit outsourcing or other prohibited nonaudit services to the public company audit client. The SEC's final rules generally become effective on May 6, 2003, although there is a one-year transition period if the accountant is performing prohibited nonaudit services and external audit services for a public

14. 15 USC 78*l* and 78o(d).

15. In addition to prohibiting internal audit outsourcing, the Sarbanes-Oxley Act (15 USC 78j-1) also identifies other nonaudit services that an external auditor is prohibited from providing to a public company whose financial statements it audits. The legislative history of the act indicates that three broad principles should be considered when determining whether an auditor should be prohibited from providing a nonaudit service to an audit client. These principles are that an auditor should not (1) audit his or her own work, (2) perform management functions for the client, or (3) serve in an advocacy role for the client. To do so would impair the auditor's independence. Based on these three broad principles, the other nonaudit services that an auditor is prohibited from providing to a public company audit client include bookkeeping or other services related to the client's accounting records or financial statements; financial information systems design and implementation; appraisal or valuation services, fairness opinions, or contribution-in-kind reports; actuarial services; management or human resources functions; broker or dealer, investment adviser, or investment banking services; legal services and expert services unrelated to the audit; and any other service determined to be impermissible by the PCAOB.

company pursuant to a contract in existence on May 6, 2003. The services provided during this transition period must not have impaired the auditor's independence under the preexisting independence requirements of the SEC, the Independence Standards Board, and the AICPA. Although the SEC's pre-Sarbanes-Oxley independence requirements (issued in November 2000, effective August 2002) did not prohibit the outsourcing of internal audit services to a public company's independent public accountant, they did place conditions and limitations on internal audit outsourcing.

Depository institutions subject to the annual audit and reporting requirements of section 36 of the FDI Act. Under section 36, as implemented by part 363 of the FDIC's regulations, each FDIC-insured depository institution with total assets of $500 million or more is required to have an annual audit performed by an independent public accountant.[16] The part 363 guidelines address the qualifications of an independent public accountant engaged by such an institution by stating that "[t]he independent public accountant should also be in compliance with the AICPA's *Code of Professional Conduct* and meet the independence requirements and interpretations of the SEC and its staff."[17]

Thus, the guidelines provide for each FDIC-insured depository institution with $500 million or more in total assets, whether or not it is a public company, and its external auditor to comply with the SEC's auditor independence requirements that are in effect during the period covered by the audit. These requirements include the nonaudit-service prohibitions and audit committee preapproval requirements implemented by the SEC's January 2003 auditor independence rules once these rule come into effect.[18]

Institutions not subject to section 36 of the FDI Act that are neither public companies nor subsidiaries of public companies. The agencies have long encouraged each institution not subject to section 36 of the FDI Act that is neither a public company nor a subsidiary of a public company[19] to have its financial statements audited by an independent public accountant.[20] The agencies also encourage each such institution to follow the internal audit outsourcing prohibition in the Sarbanes-Oxley Act, as discussed above for institutions that are public companies.

As previously mentioned, some institutions seek to enhance the quality of their control environment by obtaining the services of an outsourcing vendor who can critically assess their internal control system and recommend improvements. The agencies believe that a small nonpublic institution with less complex operations and limited staff can, in certain circumstances, use the same accounting firm to perform both an external audit and some or all of the institution's internal audit activities. These circumstances include, but are not limited to, situations in which—

- splitting the audit activities poses significant costs or burden;
- persons with the appropriate specialized knowledge and skills are difficult to locate and obtain;
- the institution is closely held and investors are not solely reliant on the audited financial statements to understand the financial position and performance of the institution; and
- the outsourced internal audit services are limited in either scope or frequency.

In circumstances such as these, the agencies view an internal audit outsourcing arrangement between a small nonpublic institution and its external auditor as not being inconsistent with their safety-and-soundness objectives for the institution.

16. 12 CFR 363.3(a). (See FDIC Financial Institutions Letter FIL-17-2003 (Corporate Governance, Audits, and Reporting Requirements), attachment II, March 5, 2003.)

17. Appendix A to part 363, Guidelines and Interpretations, paragraph 14, Independence.

18. If a depository institution subject to section 36 and part 363 satisfies the annual independent audit requirement by relying on the independent audit of its parent holding company, once the SEC's January 2003 regulations prohibiting an external auditor from performing internal audit outsourcing services for an audit client take effect May 6, 2003, or May 6, 2004, depending on the circumstances, the holding company's external auditor cannot perform internal audit outsourcing work for that holding company or the subsidiary institution.

19. FDIC-insured depository institutions with less than $500 million in total assets are not subject to section 36 of the FDI Act. Section 36 does not apply directly to holding companies but provides that, for an insured depository institution that is a subsidiary of a holding company, the audited financial statements requirement and certain of the statute's other requirements may be satisfied by the holding company.

20. See, for example, the 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Institutions.

When a small nonpublic institution decides to hire the same firm to perform internal and external audit work, the audit committee and the external auditor should pay particular attention to preserving the independence of both the internal and external audit functions. Furthermore, the audit committee should document both that it has preapproved the internal audit outsourcing to its external auditor and has considered the independence issues associated with this arrangement.[21] In this regard, the audit committee should consider the independence standards described in parts I and II of the policy statement, the AICPA guidance discussed below, and the broad principles that the auditor should not perform management functions or serve in an advocacy role for the client.

Accordingly, the agencies will not consider an auditor who performs internal audit outsourcing services for a small nonpublic audit client to be independent unless the institution and its auditor have adequately addressed the associated independence issues. In addition, the institution's board of directors and management must retain ownership of and accountability for the internal audit function and provide active oversight of the outsourced internal audit relationship.

A small nonpublic institution may be required by another law or regulation, an order, or another supervisory action to have its financial statements audited by an independent public accountant. In this situation, if warranted for safety-and-soundness reasons, the institution's primary federal regulator may require that the institution and its independent public accountant comply with the auditor-independence requirements of the act.[22]

AICPA guidance. As noted above, the independent public accountant for a depository institution subject to section 36 of the FDI Act also should be in compliance with the AICPA's *Code of Professional Conduct.* This code includes professional ethics standards, rules, and interpretations that are binding on all certified public accountants (CPAs) who are members of the AICPA in order for the member to remain in good standing. Therefore, this code applies to each member CPA who provides audit services to an institution, regardless of whether the institution is subject to section 36 or is a public company.

The AICPA has issued guidance indicating that a member CPA would be deemed not independent of his or her client when the CPA acts or appears to act in a capacity equivalent to a member of the client's management or as a client employee. The AICPA's guidance includes illustrations of activities that would be considered to compromise a CPA's independence. Among these are activities that involve the CPA authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the client. For additional details, refer to Interpretation 101-3, Performance of Other Services, and Interpretation 101-13, Extended Audit Services, in the AICPA's *Code of Professional Conduct*.

Examination Guidance (Part IV)

Review of the Internal Audit Function and Outsourcing Arrangements

Examiners should have full and timely access to an institution's internal audit resources, including personnel, workpapers, risk assessments, work plans, programs, reports, and budgets. A delay may require examiners to widen the scope of their examination work and may subject the institution to follow-up supervisory actions.

Examiners should assess the quality and scope of an institution's internal audit function, regardless of whether it is performed by the institution's employees or by an outsourcing vendor. Specifically, examiners should consider whether—

- the internal audit function's control risk assessment, audit plans, and audit programs are appropriate for the institution's activities;
- the internal audit activities have been adjusted for significant changes in the institution's environment, structure, activities, risk exposures, or systems;
- the internal audit activities are consistent with the long-range goals and strategic direction of the institution and are responsive to its internal control needs;
- the audit committee promotes the internal audit manager's impartiality and indepen-

21. If a small nonpublic institution is considering having its external auditor perform other nonaudit services, its audit committee may wish to discuss the implications of the performance of these services on the auditor's independence.

22. 15 USC 78j-1.

dence by having him or her directly report audit findings to it;
- the internal audit manager is placed in the management structure in such a way that the independence of the function is not impaired;
- the institution has promptly responded to significant identified internal control weaknesses;
- the internal audit function is adequately managed to ensure that audit plans are met, programs are carried out, and the results of audits are promptly communicated to senior management and members of the audit committee and board of directors;
- workpapers adequately document the internal audit work performed and support the audit reports;
- management and the board of directors use reasonable standards, such as the IIA's *Standards for the Professional Practice of Internal Auditing*, when assessing the performance of internal audit; and
- the audit function provides high-quality advice and counsel to management and the board of directors on current developments in risk management, internal control, and regulatory compliance.

The examiner should assess the competence of the institution's internal audit staff and management by considering the education, professional background, and experience of the principal internal auditors. In addition, when reviewing outsourcing arrangements, examiners should determine whether—

- the arrangement maintains or improves the quality of the internal audit function and the institution's internal control;
- key employees of the institution and the outsourcing vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the outsourcing vendor are to be addressed;
- the scope of the outsourced work is revised appropriately when the institution's environment, structure, activities, risk exposures, or systems change significantly;
- the directors have ensured that the outsourced internal audit activities are effectively managed by the institution;
- the arrangement with the outsourcing vendor satisfies the independence standards described in this policy statement and thereby preserves the independence of the internal audit function, whether or not the vendor is also the institution's independent public accountant; and
- the institution has performed sufficient due diligence to satisfy itself of the vendor's competence before entering into the outsourcing arrangement and has adequate procedures for ensuring that the vendor maintains sufficient expertise to perform effectively throughout the arrangement.

Examination concerns about the adequacy of the internal audit function. If the examiner concludes that the institution's internal audit function, whether or not it is outsourced, does not sufficiently meet the institution's internal audit needs; does not satisfy the Interagency Guidelines Establishing Standards for Safety and Soundness, if applicable; or is otherwise inadequate, he or she should determine whether the scope of the examination should be adjusted. The examiner should also discuss his or her concerns with the internal audit manager or other person responsible for reviewing the system of internal control. If these discussions do not resolve the examiner's concerns, he or she should bring these matters to the attention of senior management and the board of directors or audit committee. If the examiner finds material weaknesses in the internal audit function or the internal control system, he or she should discuss them with appropriate agency staff in order to determine the appropriate actions the agency should take to ensure that the institution corrects the deficiencies. These actions may include formal and informal enforcement actions.

The institution's management and composite ratings should reflect the examiner's conclusions regarding the institution's internal audit function. The report of examination should contain comments concerning the adequacy of this function, significant issues or concerns, and recommended corrective actions.

Concerns about the independence of the outsourcing vendor. An examiner's initial review of an internal audit outsourcing arrangement, including the actions of the outsourcing vendor, may raise questions about the institution's and its vendor's adherence to the independence standards described in parts I and II of the policy statement, whether or not the vendor is an accounting firm, and in part III if the vendor provides both external and internal audit services to the institution. In such cases, the exam-

iner first should ask the institution and the outsourcing vendor how the audit committee determined that the vendor was independent. If the vendor is an accounting firm, the audit committee should be asked to demonstrate how it assessed that the arrangement has not compromised applicable SEC, PCAOB, AICPA, or other regulatory standards concerning auditor independence. If the examiner's concerns are not adequately addressed, the examiner should discuss the matter with appropriate agency staff prior to taking any further action.

If the agency staff concurs that the independence of the external auditor or other vendor appears to be compromised, the examiner will discuss his or her findings and the actions the agency may take with the institution's senior management, board of directors (or audit committee), and the external auditor or other vendor. In addition, the agency may refer the external auditor to the state board of accountancy, the AICPA, the SEC, the PCAOB, or other authorities for possible violations of applicable independence standards. Moreover, the agency may conclude that the institution's external auditing program is inadequate and that it does not comply with auditing and reporting requirements, including sections 36 and 39 of the FDI Act and related guidance and regulations, if applicable. *Issued jointly by the Board, FDIC, OCC, and OTS on March 17, 2003.*

SUPPLEMENTAL POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING

The Federal Reserve issued this January 23, 2013, policy statement to supplement the guidance in the 2003 "Interagency Policy Statement on the Internal Audit Function and Its Outsourcing" (referred to as the 2003 Policy Statement).[23] Federal Reserve staff has identified areas for improving regulated institutions' internal audit functions. This supplemental policy statement addresses the characteristics, governance, and operational effectiveness of an institution's internal audit function. Further, this statement reflects certain changes in banking regulations that have occurred since the issuance of the 2003 Policy Statement. The Federal Reserve is providing this supplemental guidance to enhance regulated institutions' internal audit practices and to encourage them to adopt professional audit standards and other authoritative guidance, including those issued by the Institute of Internal Auditors (IIA).[24]

This supplemental statement applies to supervised institutions with greater than $10 billion in total consolidated assets, including state member banks, domestic bank and savings and loan holding companies, and U.S. operations of foreign banking organizations.[25] This supplemental guidance is also consistent with the objectives of the Federal Reserve's consolidated supervision framework for large financial institutions with total consolidated assets of $50 billion or more, which promotes an independent internal audit function as an essential element for enhancing the resiliency of supervised institutions.[26]

Overview—Assessment of the Effectiveness of the Internal Audit Function

The degree to which an institution implements the internal audit practices outlined in this policy statement will be considered in the Federal Reserve's supervisory assessment of the effectiveness of an institution's internal audit function as well as its safety and soundness and compliance with consumer laws and regulations. Moreover, the overall effectiveness of an institution's internal audit function will influence the ability of the Federal Reserve to rely upon the work of an institution's internal audit function.

This supplemental policy statement builds upon the 2003 Policy Statement, which remains in effect, and follows the same organizational structure, with a new section entitled "Enhanced

23. Refer to SR-03-5, "Amended Interagency Guidance on the Internal Audit Function and Its Outsourcing."

24. In this guidance, references have been provided to the IIA's International Standards for the Professional Practice of Internal Auditing (Standards). Refer to the IIA website at https://na.theiia.org/standards-guidance/pages/standards-and-guidance-ippf.aspx.

25. Section 4 of this document, however, clarifies certain changes to the Federal Deposit Insurance Corporation regulation (12 CFR part 363) on independence standards for independent public accountants at insured depository institutions with total assets of $500 million or more, which were adopted pursuant to 2009 amendments to section 36 of the FDI Act.

26. Refer to SR-12-17/CA letter 12-14, "Consolidated Supervision Framework for Large Financial Institutions."

Internal Audit Practices" and updates to Parts I-IV of the 2003 Policy Statement. Refer to SR-13-1/CA13-1 and its attachment. To avoid historical references and duplication some introductory paragraphs and other small phrases are omitted from the policy statement here, as indicated by a line of asterisks.

* * * * * *

SUPPLEMENTAL POLICY GUIDANCE

Enhanced Internal Audit Practices

An institution's internal audit function should incorporate the following enhanced practices into their overall processes:

Risk Analysis

Internal audit should analyze the effectiveness of all critical risk-management functions both with respect to individual risk dimensions (for example, credit risk), and an institution's overall risk-management function. The analysis should focus on the nature and extent of monitoring compliance with established policies and processes and applicable laws and regulations within the institution as well as whether monitoring processes are appropriate for the institution's business activities and the associated risks.

Thematic Control Issues

Internal audit should identify thematic macro control issues as part of its risk-assessment processes and determine the overall impact of such issues on the institution's risk profile. Additional audit coverage would be expected in business activities that present the highest risk to the institution. Internal audit coverage should reflect the identification of thematic macro control issues across the firm in all auditable areas. Internal audit should communicate thematic macro control issues to senior management and the audit committee.

In addition, internal audit should identify patterns of thematic macro control issues, determine whether additional audit coverage is required, communicate such control deficiencies to senior management and the audit committee, and ensure management establishes effective remediation mechanisms.

Challenging Management and Policy

Internal audit should challenge management to adopt appropriate policies and procedures and effective controls. If policies, procedures, and internal controls are ineffective or insufficient in a particular line of business or activity, internal audit should report specific deficiencies to senior management and the audit committee with recommended remediation. Such recommendations may include restricting business activity in affected lines of business until effective policies, procedures, and controls are designed and implemented. Internal audit should monitor management's corrective action and conduct a follow-up review to confirm that the recommendations of both internal audit and the audit committee have been addressed.

Infrastructure

When an institution designs and implements infrastructure enhancements, internal audit should review significant changes and notify management of potential internal control issues. In particular, internal audit should ensure that existing, effective internal controls (for example, software applications and management information system reporting) are not rendered ineffective as a result of infrastructure changes unless those controls are compensated for by other improvements to internal controls.

Risk Tolerance

Internal audit should understand risks faced by the institution and confirm that the board of directors and senior management are actively involved in setting and monitoring compliance with the institution's risk tolerance limits. Internal audit should evaluate the reasonableness of established limits and perform sufficient testing to ensure that management is operating within these limits and other restrictions.

Governance and Strategic Objectives

Internal audit should evaluate governance at all management levels within the institution, including at the senior management level, and within all significant business lines. Internal audit should also evaluate the adequacy and effectiveness of controls to respond to risks within the organization's governance, operations, and information systems in achieving the organization's strategic objectives. Any concerns should be communicated by internal audit to the board of directors and senior management.

Internal Audit Function *(Part I of the 2003 Policy Statement)*

The primary objectives of the internal audit function are to examine, evaluate, and perform an independent assessment of the institution's internal control system, and report findings back to senior management and the institution's audit committee. An effective internal audit function within a financial institution is a vital means for an institution's board of directors to maintain the quality of the internal control environment and risk-management systems.

The guidance set forth in this section supplements the existing guidance in the 2003 Policy Statement by strongly encouraging internal auditors to adhere to professional standards, such as the IIA guidance. Furthermore, this section clarifies certain aspects of the IIA guidance and provides practices intended to increase the safety and soundness of institutions.

Attributes of Internal Audit

Independence. Internal audit is an independent function that supports the organization's business objectives and evaluates the effectiveness of risk management, control, and governance processes. The 2003 Policy Statement addressed the structure of an internal audit function, noting that it should be positioned so that an institution's board of directors has confidence that the internal audit function can be impartial and not unduly influenced by managers of day-to-day operations. Thus, the member of management responsible for the internal audit function (hereafter referred to as the chief audit executive or CAE)[27] should have no responsibility for operating the system of internal control and should report functionally to the audit committee. A reporting arrangement may be used in which the CAE is functionally accountable and reports directly to the audit committee on internal audit matters (that is, the audit plan, audit findings, and the CAE's job performance and compensation) and reports administratively to another senior member of management who is not responsible for operational activities reviewed by internal audit. When there is an administrative reporting of the CAE to another member of senior management, the objectivity of internal audit is served best when the CAE reports administratively to the chief executive officer (CEO).

If the CAE reports administratively to someone other than the CEO, the audit committee should document its rationale for this reporting structure, including mitigating controls available for situations that could adversely impact the objectivity of the CAE. In such instances, the audit committee should periodically (at least annually) evaluate whether the CAE is impartial and not unduly influenced by the administrative reporting line arrangement. Further, conflicts of interest for the CAE and all other audit staff should be monitored at least annually with appropriate restrictions placed on auditing areas where conflicts may occur.

For foreign banking organizations (FBOs), the internal audit function for the U.S. operations of an FBO should have appropriate independent oversight for the total assets of U.S. operations.[28] When there is a resident U.S. audit function, the CAE of the U.S. audit function should report directly to senior officials of the internal audit department at the head office such as the global CAE. If the FBO has separate U.S. subsidiaries, oversight may be provided by a U.S. based audit committee that meets U.S. public company standards for independence or by the foreign parent company's internal audit function.

Professional competence and staffing. Internal audit staff should have the requisite collective

27. More recently, this title is used to refer to the person in charge of the internal audit function. An institution may not have a person at the management level of CAE and instead may have an internal audit manager.

28. This is defined as the combined total assets of U.S. operations, net of all intercompany assets and claims on U.S.-domiciled affiliates.

skill levels to audit all areas of the institution. Therefore, auditors should have a wide range of business knowledge, demonstrated through years of audit and industry-specific experience, educational background, professional certifications, training programs, committee participation, professional associations, and job rotational assignments. Internal audit should assign staff to audit assignments based on areas of expertise and, when feasible, rotate staff within the audit function.

Internal audit management should perform knowledge-gap assessments at least annually to evaluate whether current staff members have the knowledge and skills commensurate with the institution's strategy and operations. Management feedback surveys and internal or external quality assurance findings are useful tools to identify and assess knowledge gaps. Any identified knowledge gaps should be filled and may be addressed through targeted staff hires, training, business line rotation programs, and outsourcing arrangements. The internal audit function should have an effective staff training program to advance professional development and should have a process to evaluate and monitor the quality and appropriateness of training provided to each auditor. Internal auditors generally receive a minimum of forty hours of training in a given year.

Objectivity and ethics. Internal auditors should be objective, which means performing assignments free from bias and interference. A major characteristic of objectivity is that the CAE and all internal audit professional staff avoid any conflicts of interest.[29] For their first year in the internal audit function, internally recruited internal auditors should not audit activities for which they were previously responsible. Moreover, compensation schemes should not provide incentives for internal auditors to act contrary to the attributes and objectives of the internal audit function.[30] While an internal auditor may recommend internal control standards or review management's procedures before implementation, objectivity requires that the internal auditor not be responsible for the design, installation, procedures development, or operations of the institution's internal control systems.

An institution's internal audit function should have a code of ethics that emphasizes the principles of objectivity, competence, confidentiality, and integrity, consistent with professional internal audit guidance such as the code of ethics established by the IIA.

Internal audit charter. Each institution should have an internal audit charter that describes the purpose, authority, and responsibility of the internal audit function. An audit charter should include the following critical components:

- The objectives and scope of the internal audit function;
- The internal audit function's management reporting position within the organization, as well as its authority and responsibilities;
- The responsibility and accountability of the CAE; and
- The internal audit function's responsibility to evaluate the effectiveness of the institution's risk management, internal controls, and governance processes.

The charter should be approved by the audit committee of the institution's board of directors. The charter should provide the internal audit function with the authorization to access the institution's records, personnel, and physical properties relevant to the performance of internal audit procedures, including the authority to examine any activities or entities. Periodically, the CAE should evaluate whether the charter continues to be adequate, requesting the approval of the audit committee for any revisions. The charter should define the criteria for when and how the internal audit function may outsource some of its work to external experts.

Corporate Governance Considerations

Board of directors and senior management responsibilities. The board of directors and senior management are responsible for ensuring that the institution has an effective system of internal controls. As indicated in the 2003 Policy Statement, this responsibility cannot be delegated to others within the institution or to external parties. Further, the board of directors and senior management are responsible for ensuring that internal controls are operating effectively.

29. IIA standards define conflict of interest as a situation in which an internal auditor, who is in a position of trust, has a competing professional or personal interest. Such competing interests can make it difficult for the individual to fulfill his or her duties impartially.

30. IIA standards have additional examples of "conflict of interest" for consideration.

Audit committee responsibilities. An institution's audit committee is responsible for establishing an appropriate internal audit function and ensuring that it operates adequately and effectively. The audit committee should be confident that the internal audit function addresses the risks and meets the demands posed by the institution's current and planned activities. Moreover, the audit committee is expected to retain oversight responsibility for any aspects of the internal audit function that are outsourced to a third party.

The audit committee should provide oversight to the internal audit function. Audit committee meetings should be on a frequency that facilitates this oversight and generally should be held four times a year at a minimum, with additional meetings held by audit committees of larger financial institutions. Annually, the audit committee should review and approve internal audit's charter, budget and staffing levels, and the audit plan and overall risk-assessment methodology. The committee approves the CAE's hiring, annual performance evaluation, and compensation.

The audit committee and its chairperson should have ongoing interaction with the CAE separate from formally scheduled meetings to remain current on any internal audit department, organizational, or industry concerns. In addition, the audit committee should have executive sessions with the CAE without members of senior management present as needed.

The audit committee should receive appropriate levels of management information to fulfill its oversight responsibilities. At a minimum, the audit committee should receive the following data with respect to internal audit:

- Audit results with a focus on areas rated less than satisfactory;
- Audit plan completion status and compliance with report issuance timeframes;
- Audit plan changes, including the rationale for significant changes;
- Audit issue information, including aging, past-due status, root-cause analysis, and thematic trends;
- Information on higher-risk issues indicating the potential impact, root cause, and remediation status;
- Results of internal and external quality assurance reviews;
- Information on significant industry and institution trends in risks and controls;
- Reporting of significant changes in audit staffing levels;
- Significant changes in internal audit processes, including a periodic review of key internal audit policies and procedures;
- Budgeted audit hours versus actual audit hours;
- Information on major projects; and
- Opinion on the adequacy of risk-management processes, including effectiveness of management's self-assessment and remediation of identified issues (at least annually).

Role of the chief audit executive. In addition to communicating and reporting to the audit committee on audit-related matters, the CAE is responsible for developing and maintaining a quality assurance and improvement program that covers all aspects of internal audit activity, and for continuously monitoring the effectiveness of the audit function. The CAE and/or senior staff should effectively manage and monitor all aspects of audit work on an ongoing basis, including any audit work that is outsourced.[31]

The Adequacy of the Internal Audit Function's Processes

Internal audit should have an understanding of the institution's strategy and operating processes as well as the potential impact of current market and macroeconomic conditions on the financial institution. Internal audit's risk-assessment methodology is an integral part of the evaluation of overall policies, procedures, and controls at the institution and the development of a plan to test those processes.

Audit methodology. Internal audit should ensure that it has a well-developed risk-assessment methodology that drives its risk-assessment process. The methodology should include an analysis of cross-institutional risk and thematic control issues and address its processes and procedures for evaluating the effectiveness of risk management, control, and governance processes. The methodology should also address the role of continuous monitoring in determining and evaluating risk, as well as internal

31. The ongoing review of audit work should include risk assessments of audit entities and elements, scope documents, audit programs, detailed audit procedures and steps (including sampling methodologies), audit work papers, audit findings, and monitoring of the timely and effective resolution of audit issues.

audit's process for incorporating other risk identification techniques that the institution's management utilizes such as a risk and control self-assessment (RCSA). The components of an effective methodology should support the internal audit function's assessment of the control environment, beginning with an evaluation of the audit universe.

Audit universe. Internal audit should have effective processes to identify all auditable entities within the audit universe. The number of auditable entities will depend upon whether entities are captured at individual department levels or at other aggregated organizational levels. Internal audit should use its knowledge of the institution to determine whether it has identified all auditable entities and may use the general ledger, cost centers, new product approval processes, organization charts, department listings, knowledge of the institution's products and services, major operating and application systems, significant laws and regulations, or other data. The audit universe should be documented and reviewed periodically as significant organizational changes occur or at least during the annual audit planning process.

Internal audit risk assessment. A risk assessment should document the internal audit staff's understanding of the institution's significant business activities and the associated risks. These assessments typically analyze the risks inherent in a given business line or process, the mitigating control processes, and the resulting residual risk exposure to the institution.

A comprehensive risk assessment should effectively analyze the key risks (and the critical risk-management functions) within the institution and prioritize audit entities within the audit universe. The risk-assessment process should be well documented and dynamic, reflecting changes to the system of internal controls, infrastructure, work processes, and new or changed business lines or laws and regulations. The risk assessments should also consider thematic control issues, risk tolerance, and governance within the institution. Risk assessments should be revised in light of changing market conditions or laws and regulations and updated during the year as changes are identified in the business activities of the institution or observed in the markets in which the institution operates, but no less than annually. When the risk assessment indicates a change in risk, the audit plan should be reviewed to determine whether the planned audit coverage should be increased or decreased to address the revised assessment of risk.

Risk assessments should be formally documented and supported with written analysis of the risks.[32] There should be risk assessments for critical risk-management functions within the institution. Risk assessments may be quantitative or qualitative and may include factors such as the date of the last audit, prior audit results, the impact and likelihood of an event occurring, and the status of external vendor relationships. A management RCSA, if performed, may be considered by the internal audit function in developing its independent risk assessment. The internal audit risk assessment should also include a specific rationale for the overall auditable entity risk score. The overall disposition of the risk assessment should be summarized with consideration given to key performance or risk indicators and prior audit results. A high-level summary or discussion of the risk-assessment results should be provided to the audit committee and include the most significant risks facing the institution as well as how these risks have been addressed in the internal audit plan.

Internal audit plan. Internal audit should develop and periodically revise its comprehensive audit plan and ensure that audit coverage for all identified, auditable entities within the audit universe is appropriate for the size and complexity of the institution's activities. This should be accomplished either through a multiyear plan approach, with the plan revised annually, or through an approach that utilizes a framework to evaluate risks annually focusing on the most significant risks. In the latter approach, there should be a mechanism in place to identify when a significant risk will not be audited in the specified timeframe and a requirement to notify the audit committee and seek its approval of any exception to the framework. Generally, common practice for institutions with defined audit cycles is to follow either a three- or four-year audit cycle; high-risk areas should be audited at least every twelve to eighteen months.[33]

32. For example, risks include credit, market, operational, liquidity, compliance, IT, fraud, legal, regulatory, and strategic.

33. Regardless of the institution's practice, particular care should be taken to ensure that higher-risk elements are reviewed with an appropriate frequency, and not obscured due to their inclusion in a lower risk-rated audit entity.

The internal audit plan should consider the risk assessment and internal audit's approach to audit coverage should be appropriate based on the risk assessment. An effective plan covers individual business areas and risk disciplines as well as cross-functional and cross-institutional areas.

The audit planning process should be dynamic, allowing for change when necessary. The process should include a process for modifying the internal audit plan to incorporate significant changes that are identified either through continuous monitoring or during an audit. Any significant changes should be clearly documented and included in quarterly communications to the audit committee. Critical data to be reported to the audit committee should include deferred or cancelled audits rated high-risk and other significant additions or deletions. Significant changes to audit budgets and timeliness for the completion of audits should be reported to the audit committee with documented rationale.

Internal audit continuous monitoring. Internal audit is encouraged to utilize formal continuous monitoring practices as part of the function's risk-assessment processes to support adjustments to the audit plan or universe as they occur. Continuous monitoring can be conducted by an assigned group or individual internal auditors. An effective continuous monitoring process should include written standards to ensure consistent application of processes throughout the organization.

Continuous monitoring results should be documented through a combination of metrics, management reporting, periodic audit summaries, and updated risk assessments to substantiate that the process is operating as designed. Critical issues identified through the monitoring process should be communicated to the audit committee. Computer-assisted auditing techniques are useful tools to highlight issues that warrant further consideration within a continuous monitoring process.

Internal Audit Performance and Monitoring Processes

Performance. Detailed guidance related to the performance of an internal audit should be documented in the audit manual[34] and work programs to ensure that audit execution is consistent across the audit function. Internal audit policies and procedures should be designed to ensure that audits are executed in a high-quality manner, their results are appropriately communicated, and issues are monitored and appropriately resolved. In performing internal audit work, an institution should consider the following.

- *Internal audit scope:* During the audit planning process, internal audit should analyze the auditable entity's specific risks, mitigating controls, and level of residual risk. The information gathered during the audit planning phase should be used to determine the scope and specific audit steps that should be performed to test the adequacy of the design and operating effectiveness of control processes.

- *Internal audit work papers:* Work papers document the work performed, observations and analyses made, and support for the conclusions and audit results. The work papers should contain sufficient information regarding any scope or audit program modifications and waiver of issues not included in the final report. Work papers also should document the specific sampling methodology, including minimum sample sizes, and the rationale for such methodology. The work papers should contain information that reflects all phases of the audit process including planning, fieldwork, reporting, and issues tracking and follow-up. On an ongoing basis, a comprehensive supervisory review should be performed on all audit work, including any outsourced internal audit procedures.[35]

- *Audit report:* Internal audit should have effective processes to ensure that issues are communicated throughout the institution and audit issues are addressed in a timely manner. The audit report should include an executive summary that describes the auditable area, audit's conclusions, the rationale for those conclusions, and key issues. Most audit reports also include management's action plans to address

34. To facilitate effective, efficient, and consistent practice within the internal audit department, an institution should develop an audit manual that includes comprehensive policies and procedures and is made available to all internal audit staff. The manual should be updated as needed.

35. An experienced audit manager should perform this review.

audit findings. To ensure that identified issues are addressed in a timely manner, reports should be issued to affected business areas, senior management, and the audit committee within an appropriate timeframe after the completion of field work. Compliance with issuance timeframes should be monitored and reported periodically to the audit committee. At a minimum, internal audit should ensure that management considers the level and significance of the risk when assigning resources to address and remediate issues. Management should appropriately document the action plans either within the audit report or separately.

- *Internal audit issues tracking:* Internal audit should have effective processes in place to track and monitor open audit issues and to follow-up on such issues. The timely remediation of open audit issues is an essential component of an organization's risk reduction efforts. Internal audit and the responsible management should discuss and agree to an appropriate resolution date, based on the level of work necessary to complete remediation processes. When an issue owner indicates that work to close an issue is completed, the internal audit function should perform validation work prior to closing the issue. The level of validation necessary may vary based on the issue's risk level. For higher-risk issues, internal audit should perform and document substantive testing to validate that the issue has been resolved. Issues should be tested over an appropriate period of time to ensure the sustainability of the remediation.

Retrospective review processes. When an adverse event occurs at an institution (for example, fraud or a significant loss), management should conduct a post-mortem and ''lessons learned'' analysis. In these situations, internal audit should ensure that such a review takes place and appropriate action is taken to remediate identified issues. The internal audit function should evaluate management's analysis of the reasons for the event and whether the adverse event was the result of a control breakdown or failure, and identify the measures that should be put in place to prevent a similar event from occurring in the future. In certain situations, the internal audit function should conduct its own post-mortem and a ''lessons learned'' analysis outlining the remediation procedures necessary to detect, correct, and/or prevent future internal control breakdowns (including improvements in internal audit processes).

Quality assurance and improvement program. A well-designed, comprehensive quality assurance program should ensure that internal audit activities conform to the IIA's professional standards and the institution's internal audit policies and procedures. The program should include both internal and external quality assessments.

The internal audit function should develop and document its internal assessment program to promote and assess the quality and consistency of audit work across all audit groups with respect to policies, procedures, audit performance, and work papers. The quality assurance review should be performed by someone independent of the audit work being reviewed. Conclusions reached and recommendations for appropriate improvement in internal audit process or staff training should be implemented by the CAE through the quality assurance and improvement program. Action plan progress should be monitored and subsequently closed after a period of sustainability. Each institution should conduct an internal quality assessment annually and the CAE should report the results and status of internal assessments to senior management and the audit committee at least annually.

The IIA recommends that an external quality assessment of internal audit be performed by a qualified independent party at least once every five years. The review should address compliance with the IIA's definition of internal auditing, code of ethics, and standards, as well as with the internal audit function's charter, policies and procedures, and any applicable legislative and regulatory requirements. The CAE should communicate the results, planned actions, and status of remediation efforts to senior management and the audit committee.

Internal Audit Outsourcing Arrangements *(Part II of the 2003 Policy Statement)*

As stated in the 2003 Policy Statement, an institution's board of directors and senior management are charged with the overall responsibility for maintaining an effective system of internal controls. Responsibility for maintaining

an effective system of internal controls cannot be delegated to a third party. An institution that chooses to outsource audit work should ensure that the audit committee maintains ownership of the internal audit function. The institution's audit committee and CAE should provide active and effective oversight of outsourced activities. Institutions should carefully consider the oversight responsibilities that are consequential to these types of arrangements in determining appropriate staffing levels.

To distinguish its duties from those of the outsourcing vendor, the institution should have a written contract, which may take the form of an engagement letter or similar services agreement. Contracts between the institution and the vendor should include a provision stating that work papers and any related non-public confidential information and personal information must be handled by the vendor in accordance with applicable laws and regulations. An institution should periodically confirm that the vendor continues to comply with the agreed-upon confidentiality requirements, especially for long-term contracts. The audit committee should approve all significant aspects of outsourcing arrangements and should receive information on audit deficiencies in a manner consistent with that provided by the in-house audit department.

Vendor Competence

An institution should have appropriate policies and procedures governing the selection and oversight of internal audit vendors, including whether to continue with an existing outsourced arrangement. The audit committee and the CAE are responsible for the selection and retention of internal audit vendors and should be aware of factors that may impact vendors' competence and ability to deliver high-quality audit services.

Contingency Planning

An institution's contingency plan should take into consideration the extent to which the institution relies upon outsourcing arrangements. When an institution relies significantly on the resources of an internal audit service provider, the institution should have contingency procedures for managing temporary or permanent disruptions in the service in order to ensure that the internal audit function can meet its intended objectives.

Quality of Audit Work

The quality of audit work performed by the vendor should be consistent with the institution's standards of work expected to be performed by an in-house internal audit department. Further, information supplied by the vendor should provide the board of directors, its audit committee, and senior management with an accurate report on the control environment, including any changes necessary to enhance controls.

Independence Guidance for the Independent Public Accountant *(Part III of the 2003 Policy Statement)*

The following discussion supplements the discussion in Part III of the 2003 Policy Statement and addresses additional requirements regarding auditor independence for depository institutions subject to section 36 of the FDI Act (as amended in 2009).

Depository Institutions Subject to the Annual Audit and Reporting Requirements of Section 36 of the FDI Act

The July 2009 amendments to section 36 of the FDI Act (applicable to insured depository institutions with total assets of $500 million or more) require an institution's external auditor to follow the more restrictive of the independence rules issued by the AICPA, SEC, and PCAOB. In March 2003, the SEC prohibited a registered public accounting firm that is responsible for furnishing an opinion on the consolidated or separate financial statements of an audit client from providing internal audit services to that same client.[36] Therefore, by following the more restrictive independence rules, a depository institution's external auditor is precluded from performing internal audit services, either on a

36. See SEC final rule, "Strengthening the Commission's Requirements Regarding Auditor Independence," at 17 CFR parts 210, 240, 249 and 274.

co-sourced or an outsourced basis, even if the institution is not a public company.

Examination Guidance *(Part IV of the 2003 Policy Statement)*

The following discussion supplements the existing guidance in Part IV of the 2003 Policy Statement on examination guidance and discusses the overall effectiveness of an institution's internal audit function and the examiner's reliance on internal audit.

Determining the Overall Effectiveness of Internal Audit

An effective internal audit function is a vehicle to advance an institution's safety and soundness and compliance with consumer laws and regulations and is therefore considered as part of the supervisory review process. Federal Reserve examiners will make an overall determination as to whether the internal audit function and its processes are effective or ineffective and whether examiners can potentially rely upon internal audit's work as part of the supervisory review process. If internal audit's overall processes are deemed effective, examiners may be able to rely on the work performed by internal audit depending on the nature and risk of the functions subject to examination.

The supervisory assessment of internal audit and its effectiveness will consider an institution's application of the 2003 Policy Statement and this supplemental guidance. An institution's internal audit function generally would be considered effective if the institution's internal audit function structure and practices are consistent with the 2003 Policy Statement and this guidance.

Conversely, an institution's internal audit function that does not follow the enhanced practices and supplemental guidance outlined in this policy letter generally will be considered ineffective. In such a case, examiners will not rely on the institution's internal audit function.

Examiners will inform the CAE as to whether the function is deemed to be effective or ineffective. Internal audit's overall processes could be deemed effective even though some aspects of the internal audit function may require enhancements or improvements such as additional documentation with respect to specific audit processes (for example, risk assessments or work papers). In these situations, the required enhancements or improvements generally should not be a critical part of the overall internal audit function, or the function should be deemed to be ineffective.

Relying on the Work Performed by Internal Audit

Examiners may rely on internal audit at supervised institutions if internal audit was deemed effective at the most recent examination of internal audit. In examining an institution's internal audit function, examiners will supplement their examination procedures through continuous monitoring and an assessment of key elements of internal audit, including (1) the adequacy and independence of the audit committee; (2) the independence, professional competence, and quality of the internal audit function; (3) the quality and scope of the audit methodology, audit plan, and risk assessment; and (4) the adequacy of audit programs and work paper standards. On at least an annual basis, examiners should review these key elements to determine whether there have been significant changes in the internal audit infrastructure or whether there are potential concerns regarding their adequacy.

Examiners may choose to rely on the work of internal audit when internal audit's overall function and related processes are effective and when recent work was performed by internal audit in an area where examiners are performing examination procedures. For example, if an internal audit department performs internal audit work in an area where examiners might also review controls, examiners may evaluate whether they can rely on the work of internal audit (and either eliminate or reduce the testing scheduled as part of the regulatory examination processes). In high-risk areas, examiners will consider whether additional examination work is needed even where internal audit has been deemed effective and its work reliable.

* * * * * * * * * * *

(End of the January 23, 2013, Supplemental Policy Statement)

INDEPENDENCE OF INTERNAL AUDITORS

The ability of the internal audit function to achieve its audit objectives depends, in large part, on the independence maintained by audit personnel. Frequently, the independence of internal auditing can be determined by its reporting lines within the organization and by the person or level to whom these results are reported. In most circumstances, the internal audit function is under the direction of the board of directors or a committee thereof, such as the audit committee. This relationship enables the internal audit function to assist the directors in fulfilling their responsibilities.

The auditor's responsibilities should be addressed in a position description, with reporting lines delineated in personnel policy, and audit results should be documented in audit committee and board of directors' minutes. Examiners should review these documents, as well as the reporting process followed by the auditor, in order to subsequently evaluate the tasks performed by the internal audit function. The internal auditor should be given the authority necessary to perform the job, including free access to any records necessary for the proper conduct of the audit. Furthermore, internal auditors generally should not have responsibility for the accounting system, other aspects of the institution's accounting function, or any operational function not subject to independent review.

Competence of Internal Auditors

The responsibilities and qualifications of internal auditors vary depending on the size and complexity of a bank's operations and on the emphasis placed on the internal audit function by the directorate and management. In many banks, the internal audit function is performed by an individual or group of individuals whose sole responsibility is internal auditing. In other banks, particularly small ones, internal audit may be performed on a part-time basis by an officer or employee.

The qualifications discussed below should not be viewed as minimum requirements but should be considered by the examiner in evaluating the work performed by the internal auditors or audit departments. Examples of the type of qualifications an internal audit department manager should have are—

- academic credentials comparable to other bank officers who have major responsibilities within the organization,
- commitment to a program of continuing education and professional development,
- audit experience and organizational and technical skills commensurate with the responsibilities assigned, and
- oral and written communication skills.

The internal audit department manager must be properly trained to fully understand the flow of data and the underlying operating procedures. Training may come from college courses, courses sponsored by industry groups such as the Bank Administration Institute (BAI), or in-house training programs. Significant work experience in various departments of a bank also may provide adequate training. Certification as a chartered bank auditor, certified internal auditor, or certified public accountant meets educational and other professional requirements. In addition to prior education, the internal auditor should be committed to a program of continuing education, which may include attending technical meetings and seminars and reviewing current literature on auditing and banking.

The internal auditor's organizational skills should be reflected in the effectiveness of the bank's audit program. Technical skills may be demonstrated through internal audit techniques, such as internal control and other questionnaires, and an understanding of the operational and financial aspects of the organization.

In considering the competence of the internal audit staff, the examiner should review the educational and experience qualifications required by the bank for filling the positions in the internal audit department and the training available for that position. In addition, the examiner must be assured that any internal audit supervisor understands the audit objectives and procedures performed by the staff.

In a small bank, it is not uncommon to find that internal audit, whether full- or part-time, is a one-person department. The internal auditor may plan and perform all procedures personally or may direct staff borrowed from other departments. In either case, the examiner should expect, at a minimum, that the internal auditor

possesses qualifications similar to those of an audit department manager, as previously discussed.

The final measure of the competence of the internal auditor is the quality of the work performed, the ability to communicate the results of that work, and the ability to follow up on deficiencies noted during the audit work. Accordingly, the examiner's conclusions with respect to an auditor's competence should also reflect the adequacy of the audit program and the audit reports.

IMPLEMENTATION OF THE INTERNAL AUDIT FUNCTION

The annual audit plan and budgets should be set by the internal audit manager and approved by the board, audit committee, or senior management. In many organizations, the internal audit manager reports to a senior manager for administrative purposes. The senior manager appraises the audit manager's performance, and the directors or an audit committee approves the evaluation.

Risk Assessment

In setting the annual audit plan, a risk assessment should be made that documents the internal audit function's understanding of the institution's various business activities and their inherent risks. In addition, the assessment also evaluates control risk, or the potential that deficiencies in the system of internal control would expose the institution to potential loss. The assessment should be periodically updated to reflect changes in the system of internal control, work processes, business activities, or the business environment. The risk-assessment methodology of the internal audit function should identify all auditable areas, give a detailed basis for the auditors' determination of relative risks, and be consistent from one audit area to another. The risk assessment can quantify certain risks, such as credit risk, market risk, and legal risk. It can also include qualitative aspects, such as the timeliness of the last audit and the quality of management. Although there is no standard approach to making a risk assessment, it should be appropriate to the size and complexity of the institution. While smaller institutions may not have elaborate risk-assessment systems, some analysis should still be available to explain why certain areas are more frequently audited than others.

Within the risk assessment, institutions should clearly identify auditable units along business activities or product lines, depending on how the institution is managed. There should be evidence that the internal audit manager is regularly notified of new products, departmental changes, and new general ledger accounts, all of which should be factored into the audit schedule. Ratings of particular business activities or corporate functions may change with time as the internal audit function revises its method for assessing risk. These changes should be incremental. Large-scale changes in the priority of audits should trigger an investigation into the reasonableness of changes to the risk-assessment methodology.

Audit Plan

The audit plan is based on the risk assessment. The plan should include a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.

A formal, annual audit plan should be developed based on internal audit's risk assessment. The audit plan should include all auditable areas and set priorities based on the rating determined by the risk assessment. The schedule of planned audits should be approved by the board or its audit committee, as should any subsequent changes to the plan. Many organizations develop an audit plan jointly with the external auditors. In this case, the audit plan should clearly indicate what work is being performed by internal and external auditors and what aspects of internal audit work the external auditors are relying on.

Typically, the schedule of audit is cyclic; for example, high risks are audited annually, moderate risks every two years, and low risks every three years. In some cases, the audit cycle may extend beyond three years. In reviewing the annual plan, examiners should determine the appropriateness of the institution's audit cycle. Some institutions limit audit coverage of their low-risk areas. Examiners should review areas the institution has labeled "low risk" to deter-

mine if the classification is appropriate and if coverage is adequate.

Audit Manual

The internal audit department should have an audit manual that sets forth the standards of work for field auditors and audit managers to use in their assignments. A typical audit manual contains the audit unit's charter and mission, administrative procedures, workpaper-documentation standards, reporting standards, and review procedures. Individual audits should conform to the requirements of the audit manual. As a consequence, the manual should be up-to-date with respect to the audit function's mission and changes to the professional standards it follows.

Performance of Individual Audits

The internal audit manager should oversee the staff assigned to perform the internal audit work and should establish policies and procedures to guide them. The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and to assess whether internal controls are effective. While audits vary according to the objective, the area subjected to audit, the standards used as the basis for work performed, and documentation, the audit process generates some common documentation elements, as described below.

Audit Program and Related Workpapers

The audit program documents the audit's objectives and the procedures that were performed. Typically, it indicates who performed the work and who has reviewed it. Workpapers document the evidence gathered and conclusions drawn by the auditor, as well as the disposition of audit findings. The workpapers should provide evidence that the audit program adheres to the requirements specified in the audit manual.

Audit Reports

The audit report is internal audit's formal notice of its assessment of internal controls in the audited areas. The report is given to the area's managers, senior management, and directors. A typical audit report states the purpose of the audit and its scope, conclusions, and recommendations. Reports are usually prepared for each audit. In larger institutions, monthly or quarterly summaries that highlight major audit issues are prepared for senior management and the board.

EXAMINER REVIEW OF INTERNAL AUDIT

The examination procedures section describes the steps the examiner should follow when conducting a review of the work performed by the internal auditor. The examiner's review and evaluation of the internal audit function is a key element in determining the scope of the examination. In most situations, the competence and independence of the internal auditors may be reviewed on an overall basis; however, the adequacy and effectiveness of the audit program should be determined separately for each examination area.

The examiner should assess if the work performed by the internal auditor is reliable. It is often more efficient for the examiner to determine the independence or competence of the internal auditor before addressing the adequacy or effectiveness of the audit program. If the examiner concludes that the internal auditor possesses neither the independence nor the competence deemed appropriate, the examiner must also conclude that the internal audit work performed is not reliable.

The examiner should indicate in the report of examination any significant deficiencies concerning the internal audit function. Furthermore, the examiner should review with management any significant deficiencies noted in the previous report of examination to determine if these concerns have been appropriately addressed.

Program Adequacy and Effectiveness

An examiner should consider the following factors when assessing the adequacy of the internal audit program—

- scope and frequency of the work performed,
- content of the programs,
- documentation of the work performed, and
- conclusions reached and reports issued.

The scope of the internal audit program must be sufficient to attain the audit objectives. The frequency of the audit procedures performed should be based on an evaluation of the risk associated with each targeted area under audit. Among the factors that the internal auditor should consider in assessing risk are the nature of the operation of the specific assets and liabilities under review, the existence of appropriate policies and internal control standards, the effectiveness of operating procedures and internal controls, and the potential materiality of errors or irregularities associated with the specific operation.

To further assess the adequacy and effectiveness of the internal audit program, an examiner needs to obtain audit workpapers. Workpapers should contain, among other things, audit work programs and analyses that clearly indicate the procedures performed, the extent of the testing, and the basis for the conclusions reached.

Although audit work programs are an integral part of the workpapers, they are sufficiently important to deserve separate attention. Work programs serve as the primary guide to the audit procedures to be performed. Each program should provide a clear, concise description of the work required, and individual procedures should be presented logically. The detailed procedures included in the program vary depending on the size and complexity of the bank's operations and the area subject to audit. In addition, an individual audit work program may encompass several departments of the bank, a single department, or specific operations within a department. Most audit programs include procedures such as—

- surprise examinations, where appropriate;
- maintenance of control over records selected for audit;
- review and evaluation of the bank's policies and procedures and the system of internal control;
- reconciliation of detail to related control records; and
- verification of selected transactions and balances through procedures such as examination of supporting documentation, direct confirmation and appropriate follow-up of exceptions, and physical inspection.

The internal auditor should follow the specific procedures included in all work programs to reach audit conclusions that will satisfy the related audit objectives. Audit conclusions should be supported by report findings; such reports should include, when appropriate, recommendations by the internal auditor for any required remedial actions.

The examiner should also analyze the internal reporting process for the internal auditor's findings, since required changes in the bank's internal controls and operating procedures can be made only if appropriate officials are informed of the deficiencies. This means that the auditor must communicate all findings and recommendations clearly and concisely, pinpointing problems and suggesting solutions. The auditor also should submit reports as soon as practical, and the reports should be routed to those authorized to implement the suggested changes.

The final measure of the effectiveness of the audit program is a prompt and effective management response to the auditor's recommendations. The audit department should determine the reasonableness, timeliness, and completeness of management's response to their recommendations, including follow-up, if necessary. Examiners should assess management's response and follow up when the response is either incomplete or unreasonable.

EXTERNAL AUDITS

The Federal Reserve requires bank holding companies with total consolidated assets of $500 million or more to have annual independent audits. Generally, banks must have external audits for the first three years after obtaining FDIC insurance (an FDIC requirement) and upon becoming a newly chartered national bank (an OCC requirement). The SEC also has a longstanding audit requirement for all public companies, which applies to bank holding companies that are SEC registrants and to state member banks that are subject to SEC reporting requirements pursuant to the Federal Reserve's Regulation H.

For insured depository institutions with fiscal years beginning after December 31, 1992, FDICIA, through its amendments to section 36 of the FDI Act, requires annual independent audits for all FDIC-insured banks that have total assets in excess of $500 million. (See SR-94-3

and SR-96-4.) In September 1999, the Federal Financial Institutions Examination Council (FFIEC) issued an interagency policy statement on external auditing programs of banks and savings associations.[37] The policy encourages banks and savings associations that have *less than* $500 million in total assets and that are not subject to other audit requirements to adopt an external auditing program as a part of their overall risk-management process. (See the following subsection for the complete text of the interagency policy statement.)

Independent audits enhance the probability that financial statements and reports to the FRB and other financial-statement users will be accurate and will help detect conditions that could adversely affect banking organizations, the FRB, or the public. The independent audit process also subjects the internal controls and the accounting policies, procedures, and records of each banking organization to periodic review.

Banks often employ external auditors and other specialists to assist management in specialized fields, such as taxation and management information systems. External auditors and consultants often conduct in-depth reviews of the operations of specific bank departments; the reviews might focus on operational procedures, personnel requirements, or other specific areas of interest. After completing the reviews, the auditors may recommend that the bank strengthen controls or improve efficiency.

External auditors provide services at various times during the year. Financial statements are examined annually. Generally, the process commences in the latter part of the year, with the report issued as soon thereafter as possible. Other types of examinations or reviews are performed at various dates on an as-required basis.

The examiner is interested in the work performed by external auditors for three principal reasons. First, situations will arise when internal audit work is not being performed or when such work is deemed to be of limited value to the examiner. Second, the work performed by external auditors may affect the amount of testing the examiner must perform. Third, external audit reports often provide the examiner with information pertinent to the examination of the bank.

The major factors that should be considered in evaluating the work of external auditors are similar to those applicable to internal auditors, namely, the competence and independence of the auditors and the adequacy of the audit program.

The federal banking agencies view a full-scope annual audit of a bank's financial statements by an independent public accountant as preferable to other types of external auditing programs. The September 1999 policy statement recognizes that a full-scope audit may not be feasible for every small bank. It therefore encourages those banks to pursue appropriate alternatives to a full-scope audit. Small banks are also encouraged to establish an audit committee consisting of outside directors. The policy statement provides guidance to examiners on the review of external auditing programs.

The policy statement is consistent with the Federal Reserve's longstanding guidance that encourages the use of external auditing programs, and with its goals for (1) ensuring the accuracy and reliability of regulatory reports, (2) improving the quality of bank internal controls over financial reporting, and (3) enhancing the efficiency of the risk-focused examination process. The Federal Reserve adopted the FFIEC policy statement effective for fiscal years beginning on or after January 1, 2000. (See SR-99-33.)

INTERAGENCY POLICY STATEMENT ON EXTERNAL AUDITING PROGRAMS OF BANKS AND SAVINGS ASSOCIATIONS

Introduction

The board of directors and senior managers of a banking institution or savings association (institution) are responsible for ensuring that the institution operates in a safe and sound manner. To achieve this goal and meet the safety-and-soundness guidelines implementing section 39 of the Federal Deposit Insurance Act (FDI Act) (12 USC 1831p-1),[38] the institution should maintain effective systems and internal control[39] to produce reliable and accurate financial reports.

37. See 64 *Fed. Reg.* 52319 (September 28, 1999).

38. See 12 CFR 30 for national banks; 12 CFR 364 for state nonmember banks; 12 CFR 208 for state member banks; and 12 CFR 510 for savings associations.

39. This policy statement provides guidance consistent

Accurate financial reporting is essential to an institution's safety and soundness for numerous reasons. First, accurate financial information enables management to effectively manage the institution's risks and make sound business decisions. In addition, institutions are required by law[40] to provide accurate and timely financial reports (e.g., Reports of Condition and Income [call reports] and Thrift Financial Reports) to their appropriate regulatory agency. These reports serve an important role in the agencies'[41] risk-focused supervision programs by contributing to their pre-examination planning, off-site monitoring programs, and assessments of an institution's capital adequacy and financial strength. Further, reliable financial reports are necessary for the institution to raise capital. They provide data to stockholders, depositors and other funds providers, borrowers, and potential investors on the company's financial position and results of operations. Such information is critical to effective market discipline of the institution.

To help ensure accurate and reliable financial reporting, the agencies recommend that the board of directors of each institution establish and maintain an external auditing program. An external auditing program should be an important component of an institution's overall risk-management process. For example, an external auditing program complements the internal auditing function of an institution by providing management and the board of directors with an independent and objective view of the reliability of the institution's financial statements and the adequacy of its financial-reporting internal controls. Additionally, an effective external auditing program contributes to the efficiency of the agencies' risk-focused examination process. By considering the significant risk areas of an institution, an effective external auditing program may reduce the examination time the agencies spend in such areas. Moreover, it can improve the safety and soundness of an institution substantially and lessen the risk the institution poses to the insurance funds administered by the Federal Deposit Insurance Corporation (FDIC).

This policy statement outlines the characteristics of an effective external auditing program and provides examples of how an institution can use an external auditor to help ensure the reliability of its financial reports. It also provides guidance on how an examiner may assess an institution's external auditing program. In addition, this policy statement provides specific guidance on external auditing programs for institutions that are holding company subsidiaries, newly insured institutions, and institutions presenting supervisory concerns.

The adoption of a financial statement audit or other specified type of external auditing program is generally only required in specific circumstances. For example, insured depository institutions covered by section 36 of the FDI Act (12 USC 1831m), as implemented by part 363 of the FDIC's regulations (12 CFR 363), are required to have an external audit and an audit committee. Therefore, this policy statement is directed toward banks and savings associations which are exempt from part 363 (i.e., institutions with less than $500 million in total assets at the beginning of their fiscal year) or are not otherwise subject to audit requirements by order, agreement, statute, or agency regulations.

Overview of External Auditing Programs

Responsibilities of the Board of Directors

The board of directors of an institution is responsible for determining how to best obtain reasonable assurance that the institution's financial statements and regulatory reports are reliably prepared. In this regard, the board is also responsible for ensuring that its external auditing program is appropriate for the institution and adequately addresses the financial-reporting aspects of the significant risk areas and any other areas of concern of the institution's business.

To help ensure the adequacy of its internal and external auditing programs, the agencies encourage the board of directors of each institution that is not otherwise required to do so to establish an audit committee consisting entirely of outside directors.[42] However, if this is impracticable, the board should organize the

with the guidance established in the Interagency Policy Statement on the Internal Audit Function and Its Outsourcing.

40. See 12 USC 161 for national banks; 12 USC 1817a for state nonmember banks; 12 USC 324 for state member banks; and 12 USC 1464(v) for savings associations.

41. Terms are defined at the end of the policy statement.

42. Institutions with $500 million or more in total assets must establish an independent audit committee made up of outside directors who are independent of management. See 12 USC 1831m(g)(1) and 12 CFR 363.5.

audit committee so that outside directors constitute a majority of the membership.

Audit Committee

The audit committee or board of directors is responsible for identifying at least annually the risk areas of the institution's activities and assessing the extent of external auditing involvement needed over each area. The audit committee or board is then responsible for determining what type of external auditing program will best meet the institution's needs (see the descriptions under ''Types of External Auditing Programs'').

When evaluating the institution's external auditing needs, the board or audit committee should consider the size of the institution and the nature, scope, and complexity of its operations. It should also consider the potential benefits of an audit of the institution's financial statements or an examination of the institution's internal control structure over financial reporting, or both. In addition, the board or audit committee may determine that additional or specific external auditing procedures are warranted for a particular year or several years to cover areas of particularly high risk or special concern. The reasons supporting these decisions should be recorded in the committee's or board's minutes.

If, in its annual consideration of the institution's external auditing program, the board or audit committee determines, after considering its inherent limitations, that an agreed-upon procedures/state-required examination is sufficient, they should also consider whether an independent public accountant should perform the work. When an independent public accountant performs auditing and attestation services, the accountant must conduct his or her work under, and may be held accountable for departures from, professional standards. Furthermore, when the external auditing program includes an audit of the financial statements, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial statements are presented fairly, in all material respects, in accordance with generally accepted accounting principles (GAAP). When the external auditing program includes an examination of the internal control structure over financial reporting, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial-reporting process is subject to any material weaknesses.

Both the staff performing an internal audit function and the independent public accountant or other external auditor should have unrestricted access to the board or audit committee without the need for any prior management knowledge or approval. Other duties of an audit committee may include reviewing the independence of the external auditor annually, consulting with management, seeking an opinion on an accounting issue, and overseeing the quarterly regulatory reporting process. The audit committee should report its findings periodically to the full board of directors.

External Auditing Programs

Basic Attributes

External auditing programs should provide the board of directors with information about the institution's financial-reporting risk areas, e.g., the institution's internal control over financial reporting, the accuracy of its recording of transactions, and the completeness of its financial reports prepared in accordance with GAAP.

The board or audit committee of each institution at least annually should review the risks inherent in its particular activities to determine the scope of its external auditing program. For most institutions, the lending and investment-securities activities present the most significant risks that affect financial reporting. Thus, external auditing programs should include specific procedures designed to test at least annually the risks associated with the loan and investment portfolios. This includes testing of internal control over financial reporting, such as management's process to determine the adequacy of the allowance for loan and lease losses and whether this process is based on a comprehensive, adequately documented, and consistently applied analysis of the institution's loan and lease portfolio.

An institution or its subsidiaries may have other significant financial-reporting risk areas such as material real estate investments, insurance underwriting or sales activities, securities broker-dealer or similar activities (including securities underwriting and investment advisory services), loan-servicing activities, or fiduciary

activities. The external auditing program should address these and other activities the board or audit committee determines present significant financial-reporting risks to the institution.

Types of External Auditing Programs

The agencies consider an annual audit of an institution's financial statements performed by an independent public accountant to be the preferred type of external auditing program. The agencies also consider an annual examination of the effectiveness of the internal control structure over financial reporting or an audit of an institution's balance sheet, both performed by an independent public accountant, to be acceptable alternative external auditing programs. However, the agencies recognize that some institutions only have agreed-upon procedures/state-required examinations performed annually as their external auditing program. Regardless of the option chosen, the board or audit committee should agree in advance with the external auditor on the objectives and scope of the external auditing program.

Financial statement audit by an independent public accountant. The agencies encourage all institutions to have an external audit performed in accordance with generally accepted auditing standards (GAAS). The audit's scope should be sufficient to enable the auditor to express an opinion on the institution's financial statements taken as a whole.

A financial statement audit provides assurance about the fair presentation of an institution's financial statements. In addition, an audit may provide recommendations for management in carrying out its control responsibilities. For example, an audit may provide management with guidance on establishing or improving accounting and operating policies and recommendations on internal control (including internal auditing programs) necessary to ensure the fair presentation of the financial statements.

Reporting by an independent public accountant on an institution's internal control structure over financial reporting. Another external auditing program is an independent public accountant's examination and report on management's assertion on the effectiveness of the institution's internal control over financial reporting. For a smaller institution with less complex operations, this type of engagement is likely to be less costly than an audit of its financial statements or its balance sheet. It would specifically provide recommendations for improving internal control, including suggestions for compensating controls, to mitigate the risks due to staffing and resource limitations.

Such an attestation engagement may be performed for all internal controls relating to the preparation of annual financial statements or specified schedules of the institution's regulatory reports.[43] This type of engagement is performed under generally accepted standards for attestation engagements (GASAE).[44]

Balance-sheet audit performed by an independent public accountant. With this program, the institution engages an independent public accountant to examine and report only on the balance sheet. As with the audit of the financial statements, this audit is performed in accordance with GAAS. The cost of a balance-sheet audit is likely to be less than a financial-statement audit. However, under this type of program, the accountant does not examine or report on the fairness of the presentation of the

43. Since the lending and investment-securities activities generally present the most significant risks that affect an institution's financial reporting, management's assertion and the accountant's attestation generally should cover those regulatory report schedules. If the institution has trading or off-balance-sheet activities that present material financial-reporting risks, the board or audit committee should ensure that the regulatory report schedules for those activities also are covered by management's assertion and the accountant's attestation. For banks and savings associations, the lending, investment-securities, trading, and off-balance-sheet schedules consist of:

Area	*Reports of Condition and Income Schedules*	*Thrift Financial Report Schedules*
Loans and lease-financing receivables	RC-C, Part I	SC, CF
Past-due and nonaccrual loans, leases, and other assets	RC-N	PD
Allowance for credit losses	RI-B	SC, VA
Securities	RC-B	SC, SI, CF
Trading assets and liabilities	RC-D	SO, SI
Off-balance-sheet items	RC-L	SI, CMR

These schedules are not intended to address all possible risks in an institution.

44. An attestation engagement is not an audit. It is performed under different professional standards than an audit of an institution's financial statements or its balance sheet.

institution's income statement, statement of changes in equity capital, or statement of cash flows.

Agreed-upon procedures/state-required examinations. Some state-chartered depository institutions are required by state statute or regulation to have specified procedures performed annually by their directors or independent persons.[45] The bylaws of many national banks also require that some specified procedures be performed annually by directors or others, including internal or independent persons. Depending upon the scope of the engagement, the cost of agreed-upon procedures or a state-required examination may be less than the cost of an audit. However, under this type of program, the independent auditor does not report on the fairness of the institution's financial statements or attest to the effectiveness of the internal control structure over financial reporting. The findings or results of the procedures are usually presented to the board or the audit committee so that they may draw their own conclusions about the quality of the financial reporting or the sufficiency of internal control.

When choosing this type of external auditing program, the board or audit committee is responsible for determining whether these procedures meet the external auditing needs of the institution, considering its size and the nature, scope, and complexity of its business activities. For example, if an institution's external auditing program consists solely of confirmations of deposits and loans, the board or committee should consider expanding the scope of the auditing work performed to include additional procedures to test the institution's high-risk areas. Moreover, a financial statement audit, an examination of the effectiveness of the internal control structure over financial reporting, and a balance-sheet audit may be accepted in some states and for national banks in lieu of agreed-upon procedures/state-required examinations.

Other Considerations

Timing. The preferable time to schedule the performance of an external auditing program is as of an institution's fiscal year-end. However, a quarter-end date that coincides with a regulatory report date provides similar benefits. Such an approach allows the institution to incorporate the results of the external auditing program into its regulatory reporting process and, if appropriate, amend the regulatory reports.

External auditing staff. The agencies encourage an institution to engage an independent public accountant to perform its external auditing program. An independent public accountant provides a nationally recognized standard of knowledge and objectivity by performing engagements under GAAS or GASAE. The firm or independent person selected to conduct an external auditing program and the staff carrying out the work should have experience with financial-institution accounting and auditing or similar expertise and should be knowledgeable about relevant laws and regulations.

Special Situations

Holding Company Subsidiaries

When an institution is owned by another entity (such as a holding company), it may be appropriate to address the scope of its external audit program in terms of the institution's relationship to the consolidated group. In such cases, if the group's consolidated financial statements for the same year are audited, the agencies generally would not expect the subsidiary of a holding company to obtain a separate audit of its financial statements. Nevertheless, the board of directors or audit committee of the subsidiary may determine that its activities involve significant risks to the subsidiary that are not within the procedural scope of the audit of the financial statements of the consolidated entity. For example, the risks arising from the subsidiary's activities may be immaterial to the financial statements of the consolidated entity, but material to the subsidiary. Under such circumstances, the audit committee or board of the subsidiary should consider strengthening the internal audit coverage of those activities or implementing an appropriate alternative external auditing program.

45. When performed by an independent public accountant, "specified procedures" and "agreed-upon procedures" engagements are performed under standards, which are different professional standards than those used for an audit of an institution's financial statements or its balance sheet.

Newly Insured Institutions

Under the FDIC statement of policy on applications for deposit insurance, applicants for deposit insurance coverage are expected to commit the depository institution to obtain annual audits by an independent public accountant once it begins operations as an insured institution and for a limited period thereafter.

Institutions Presenting Supervisory Concerns

As previously noted, an external auditing program complements the agencies' supervisory process and the institution's internal auditing program by identifying or further clarifying issues of potential concern or exposure. An external auditing program also can greatly assist management in taking corrective action, particularly when weaknesses are detected in internal control or management information systems affecting financial reporting.

The agencies may require a financial institution presenting safety-and-soundness concerns to engage an independent public accountant or other independent external auditor to perform external auditing services.[46] Supervisory concerns may include—

- inadequate internal control, including the internal auditing program;
- a board of directors generally uninformed about internal control;
- evidence of insider abuse;
- known or suspected defalcations;
- known or suspected criminal activity;
- probable director liability for losses;
- the need for direct verification of loans or deposits;
- questionable transactions with affiliates; or
- the need for improvements in the external auditing program.

The agencies may also require that the institution provide its appropriate supervisory office with a copy of any reports, including management letters, issued by the independent public accountant or other external auditor. They also may require the institution to notify the supervisory office prior to any meeting with the independent public accountant or other external auditor at which auditing findings are to be presented.

Examiner Guidance

Review of the External Auditing Program

The review of an institution's external auditing program is a normal part of the agencies' examination procedures. An examiner's evaluation of, and any recommendations for improvements in, an institution's external auditing program will consider the institution's size; the nature, scope, and complexity of its business activities; its risk profile; any actions taken or planned by it to minimize or eliminate identified weaknesses; the extent of its internal audit program; and any compensating controls in place. Examiners will exercise judgment and discretion in evaluating the adequacy of an institution's external auditing program.

Specifically, examiners will consider the policies, processes, and personnel surrounding an institution's external auditing program in determining whether—

- the board of directors or its audit committee adequately reviews and approves external auditing program policies at least annually;
- the external auditing program is conducted by an independent public accountant or other independent auditor and is appropriate for the institution;
- the engagement letter covering external auditing activities is adequate;
- the report prepared by the auditor on the results of the external auditing program adequately explains the auditor's findings;
- the external auditor maintains appropriate independence regarding relationships with the institution under relevant professional standards;
- the board of directors performs due diligence on the relevant experience and competence of the independent auditor and staff carrying out the work (whether or not an independent public accountant is engaged); and
- the board or audit committee minutes reflect approval and monitoring of the external auditing program and schedule, including board or

46. The Office of Thrift Supervision requires an external audit by an independent public accountant for savings associations with a composite rating of 3, 4, or 5 under the Uniform Financial Institution Rating System, and on a case-by-case basis.

committee reviews of audit reports with management and timely action on audit findings and recommendations.

Access to Reports

Management should provide the independent public accountant or other auditor with access to all examination reports and written communication between the institution and the agencies or state bank supervisor since the last external auditing activity. Management also should provide the accountant with access to any supervisory memoranda of understanding, written agreements, administrative orders, reports of action initiated or taken by a federal or state banking agency under section 8 of the FDI Act (or a similar state law), and proposed or ordered assessments of civil money penalties against the institution or an institution-related party, as well as any associated correspondence. The auditor must maintain the confidentiality of examination reports and other confidential supervisory information.

In addition, the independent public accountant or other auditor of an institution should agree in the engagement letter to grant examiners access to all the accountant's or auditor's workpapers and other material pertaining to the institution prepared in the course of performing the completed external auditing program.

Institutions should provide reports[47] issued by the independent public accountant or other auditor pertaining to the external auditing program, including any management letters, to the agencies and any state authority in accordance with their appropriate supervisory office's guidance.[48] Significant developments regarding the external auditing program should be communicated promptly to the appropriate supervisory office. Examples of those developments include the hiring of an independent public accountant or other third party to perform external auditing work and a change in, or termination of, an independent public accountant or other external auditor.

Definitions

Agencies. The agencies are the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

Appropriate supervisory office. The regional or district office of the institution's primary federal banking agency responsible for supervising the institution or, in the case of an institution that is part of a group of related insured institutions, the regional or district office of the institution's federal banking agency responsible for monitoring the group. If the institution is a subsidiary of a holding company, the term "appropriate supervisory office" also includes the federal banking agency responsible for supervising the holding company. In addition, if the institution is state-chartered, the term "appropriate supervisory office" includes the appropriate state bank or savings association regulatory authority.

Audit. An examination of the financial statements, accounting records, and other supporting evidence of an institution performed by an independent certified or licensed public accountant in accordance with generally accepted auditing standards (GAAS) and of sufficient scope to enable the independent public accountant to express an opinion on the institution's financial statements as to their presentation in accordance with generally accepted accounting principles (GAAP).

Audit committee. A committee of the board of directors whose members should, to the extent possible, be knowledgeable about accounting and auditing. The committee should be responsible for reviewing and approving the institution's internal and external auditing programs or

47. The institution's engagement letter is not a "report" and is not expected to be submitted to the appropriate supervisory office unless specifically requested by that office.

48. When an institution's financial information is included in the audited consolidated financial statements of its parent company, the institution should provide a copy of the audited financial statements of the consolidated company and any other reports by the independent public accountant in accordance with their appropriate supervisory office's guidance. If several institutions are owned by one parent company, a single copy of the reports may be supplied in accordance with the guidance of the appropriate supervisory office of each agency supervising one or more of the affiliated institutions and the holding company. A transmittal letter should identify the institutions covered. Any notifications of changes in, or terminations of, a consolidated company's independent public accountant may be similarly supplied to the appropriate supervisory office of each supervising agency.

recommending adoption of these programs to the full board.

Balance-sheet audit performed by an independent public accountant. An examination of an institution's balance sheet and any accompanying footnotes performed and reported on by an independent public accountant in accordance with GAAS and of sufficient scope to enable the independent public accountant to express an opinion on the fairness of the balance-sheet presentation in accordance with GAAP.

Engagement letter. A letter from an independent public accountant to the board of directors or audit committee of an institution that usually addresses the purpose and scope of the external auditing work to be performed, period of time to be covered by the auditing work, reports expected to be rendered, and any limitations placed on the scope of the auditing work.

Examination of the internal control structure over financial reporting. See "Reporting by an independent public accountant on an institution's internal control structure over financial reporting."

External auditing program. The performance of procedures to test and evaluate high-risk areas of an institution's business by an independent auditor, who may or may not be a public accountant, sufficient for the auditor to be able to express an opinion on the financial statements or to report on the results of the procedures performed.

Financial statement audit by an independent public accountant. See Audit.

Financial statements. The statements of financial position (balance sheet), income, cash flows, and changes in equity together with related notes.

Independent public accountant. An accountant who is independent of the institution and registered or licensed to practice, and holds himself or herself out, as a public accountant, and who is in good standing under the laws of the state or other political subdivision of the United States in which the home office of the institution is located. The independent public accountant should comply with the American Institute of Certified Public Accountants' (AICPA) Code of Professional Conduct and any related guidance adopted by the Independence Standards Board and the agencies. No certified public accountant or public accountant will be recognized as independent who is not independent both in fact and in appearance.

Internal auditing. An independent assessment function established within an institution to examine and evaluate its system of internal control and the efficiency with which the various units of the institution are carrying out their assigned tasks. The objective of internal auditing is to assist the management and directors of the institution in the effective discharge of their responsibilities. To this end, internal auditing furnishes management with analyses, evaluations, recommendations, counsel, and information concerning the activities reviewed.

Outside directors. Members of an institution's board of directors who are not officers, employees, or principal stockholders of the institution, its subsidiaries, or its affiliates, and who do not have any material business dealings with the institution, its subsidiaries, or its affiliates.

Regulatory reports. These reports are the Reports of Condition and Income (call reports) for banks, Thrift Financial Reports (TFRs) for savings associations, Federal Reserve (FR) Y reports for bank holding companies, and the H-(b)11 Annual Report for thrift holding companies.

Reporting by an independent public accountant on an institution's internal control structure over financial reporting. Under this engagement, management evaluates and documents its review of the effectiveness of the institution's internal control over financial reporting in the identified risk areas as of a specific report date. Management prepares a written assertion, which specifies the criteria on which management based its evaluation about the effectiveness of the institution's internal control over financial reporting in the identified risk areas and states management's opinion on the effectiveness of internal control over this specified financial reporting. The independent public accountant is engaged to perform tests on the internal control over the specified financial reporting in order to attest to management's assertion. If the accountant concurs with management's assertion, even if the assertion discloses one or more instances of material internal control weakness, the

accountant would provide a report attesting to management's assertion.

Risk areas. Those particular activities of an institution that expose it to greater potential losses if problems exist and go undetected. The areas with the highest financial-reporting risk in most institutions generally are their lending and investment-securities activities.

Specified procedures. Procedures agreed upon by the institution and the auditor to test its activities in certain areas. The auditor reports findings and test results, but does not express an opinion on controls or balances. If performed by an independent public accountant, these procedures should be performed under generally accepted standards for attestation engagements (GASAE).

Issued by the FFIEC on September 28, 1999.

UNSAFE AND UNSOUND USE OF LIMITATION OF LIABILITY PROVISIONS IN EXTERNAL AUDIT ENGAGEMENT LETTERS

On February 9, 2006, the Federal Reserve and the other financial institution regulatory agencies (the agencies)[49] issued an interagency advisory (the advisory) to address safety-and-soundness concerns that may arise when financial institutions enter into external audit contracts (typically referred to as *engagement letters*) that limit the auditors' liability for audit services.[50] The advisory informs financial institutions'[51] boards of directors, audit committees, management, and external auditors of the safety-and-soundness implications that may arise when the financial institution enters into engagement letters that contain provisions to limit the auditors' liability. Such provisions may weaken the external auditors' objectivity, impartiality, and performance and, thus, reduce the agencies' ability to rely on audits. Therefore, certain limitation-of-liability provisions (described in the advisory) are unsafe and unsound. In addition, such provisions may not be consistent with the auditor-independence standards of the SEC, the PCAOB, and the AICPA.

The advisory does not apply to previously executed engagement letters. However, any financial institution subject to a multiyear audit engagement letter containing unsafe and unsound limitation-of-liability provisions should seek an amendment to its engagement letter to be consistent with the advisory for periods ending in 2007 or later. (See SR-06-4.)

Scope of the Advisory on Engagement Letters

The advisory applies to engagement letters between financial institutions and external auditors with respect to financial-statement audits, audits of internal control over financial reporting, and attestations on management's assessment of internal control over financial reporting (collectively, *audit* or *audits*).

The advisory does not apply to—

- nonaudit services that may be performed by financial institutions' external auditors,
- audits of financial institutions' 401(k) plans, pension plans, and other similar audits,
- services performed by accountants who are not engaged to perform financial institutions' audits (e.g., outsourced internal audits or loan reviews), and
- other service providers (e.g., software consultants or legal advisers).

While the agencies have observed several types of limitation-of-liability provisions in external audit engagement letters, this advisory applies to any agreement that a financial institution enters into with its external auditor that limits the external auditor's liability with respect to audits in an unsafe and unsound manner.

External Audits and Their Engagement Letters

A properly conducted audit provides an independent and objective view of the reliability of a financial institution's financial statements. The

49. The Board of Governors of the Federal Reserve System (Board), 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).

50. The advisory is effective for audit engagement letters issued on or after February 9, 2006.

51. As used in this advisory, the term *financial institutions* includes banks, bank holding companies, savings associations, savings and loan holding companies, and credit unions.

external auditor's objective in an audit is to form an opinion on the financial statements taken as a whole. When planning and performing the audit, the external auditor considers the financial institution's internal control over financial reporting. Generally, the external auditor communicates any identified deficiencies in internal control to management, which enables management to take appropriate corrective action. In addition, certain financial institutions are required to file audited financial statements and internal control audit or attestation reports with one or more of the agencies. The agencies encourage financial institutions not subject to mandatory audit requirements to voluntarily obtain audits of their financial statements. The FFIEC's *Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations* notes,[52] "[a]n institution's internal and external audit programs are critical to its safety and soundness." The policy also states that an effective external auditing program "can improve the safety and soundness of an institution substantially and lessen the risk the institution poses to the insurance funds administered by the FDIC."

Typically, a written engagement letter is used to establish an understanding between the external auditor and the financial institution regarding the services to be performed in connection with the financial institution's audit. The engagement letter commonly describes the objective of the audit, the reports to be prepared, the responsibilities of management and the external auditor, and other significant arrangements (for example, fees and billing). Boards of directors, audit committees, and management are encouraged to closely review all of the provisions in the audit engagement letter before agreeing to sign. As with all agreements that affect a financial institution's legal rights, the financial institution's legal counsel should carefully review audit engagement letters to help ensure that those charged with engaging the external auditor make a fully informed decision.

The advisory describes the types of objectionable limitation-of-liability provisions and provides examples.[53] Financial institutions' boards of directors, audit committees, and management should also be aware that certain insurance policies (such as error and omission policies and directors' and officers' liability policies) might not cover losses arising from claims that are precluded by limitation-of-liability provisions.

Limitation-of-Liability Provisions

The provisions of an external audit engagement letter that the agencies deem to be unsafe and unsound can be generally categorized as follows: a provision within an agreement between a client financial institution and its external auditor that effectively—

- indemnifies the external auditor against claims made by third parties;
- holds harmless or releases the external auditor from liability for claims or potential claims that might be asserted by the client financial institution, other than claims for punitive damages; or
- limits the remedies available to the client financial institution, other than punitive damages.

Collectively, these categories of provisions are referred to in this advisory as *limitation-of liability-provisions.*

Provisions that waive the right of financial institutions to seek punitive damages from their external auditor are not treated as unsafe and unsound under the advisory. Nevertheless, agreements by clients to indemnify their auditors against any third-party damage awards, including punitive damages, are deemed unsafe and unsound under the advisory. To enhance transparency and market discipline, public financial institutions that agree to waive claims for punitive damages against their external auditors may want to disclose annually the nature of these arrangements in their proxy statements or other public reports.

Many financial institutions are required to have their financial statements audited, while others voluntarily choose to undergo such audits. For example, federally insured banks with $500 million or more in total assets are required

52. See 64 *Fed. Reg.* 52319 (September 28, 1999).

53. In the majority of external audit engagement letters reviewed, the agencies did not observe provisions that limited an external auditor's liability. However, for those reviewed external audit engagement letters that did have external auditor limited-liability provisions, the agencies noted a significant increase in the types and frequency of the provisions. The provisions took many forms, which made it impractical for the agencies to provide an all-inclusive list. Examples of auditor limitation-of-liability provisions are illustrated in the advisory's appendix A, which can be found in section A.1010.1 of this manual.

to have annual independent audits.[54] Furthermore, financial institutions that are public companies[55] must have annual independent audits. The agencies rely on the results of audits as part of their assessment of a financial institution's safety and soundness.

For audits to be effective, the external auditors must be independent in both fact and appearance, and they must perform all necessary procedures to comply with auditing and attestation standards established by either the AICPA or, if applicable, the PCAOB. When financial institutions execute agreements that limit the external auditors' liability, the external auditors' objectivity, impartiality, and performance may be weakened or compromised, and the usefulness of the audits for safety-and-soundness purposes may be diminished.

By their very nature, limitation-of-liability provisions can remove or greatly weaken external auditors' objective and unbiased consideration of problems encountered in audit engagements and may diminish auditors' adherence to the standards of objectivity and impartiality required in the performance of audits. The existence of such provisions in external audit engagement letters may lead to the use of less extensive or less thorough procedures than would otherwise be followed, thereby reducing the reliability of audits. Accordingly, financial institutions should not enter into external audit arrangements that include unsafe and unsound limitation-of-liability provisions identified in the advisory, regardless of (1) the size of the financial institution, (2) whether the financial institution is public or not, or (3) whether the external audit is required or voluntary.

Auditor Independence

Currently, auditor-independence standard-setters include the SEC, PCAOB, and AICPA. Depending on the audit client, an external auditor is subject to the independence standards issued by one or more of these standard-setters. For all nonpublic financial institutions that are not required to have annual independent audits, the FDIC's rules, pursuant to part 363, require only that an external auditor meet the AICPA independence standards. The rules do not require the financial institution's external auditor to comply with the independence standards of the SEC and the PCAOB.

In contrast, for financial institutions subject to the audit requirements in part 363 of the FDIC's regulations, the external auditor should be in compliance with the AICPA's Code of Professional Conduct and meet the independence requirements and interpretations of the SEC and its staff.[56] In this regard, in a December 13, 2004, frequently asked question (FAQ) on the application of the SEC's auditor-independence rules, the SEC staff reiterated its long-standing position that when an accountant and his or her client enter into an agreement that seeks to provide the accountant immunity from liability for his or her own negligent acts, the accountant is not independent. The FAQ also stated that including in engagement letters a clause that would release, indemnify, or hold the auditor harmless from any liability and costs resulting from knowing misrepresentations by management would impair the auditor's independence.[57] The FAQ is consistent with the SEC's Codification of Financial Reporting Policies, section 602.02.f.i , "Indemnification by Client." (See section A.1010.1 of this manual.)

On the basis of the SEC guidance and the agencies' existing regulations, certain limits onauditors' liability are already inappropriate in audit engagement letters entered into by—

- public financial institutions that file reports with the SEC or with the agencies,
- financial institutions subject to part 363, and
- certain other financial institutions that are required to have annual independent audits.

In addition, certain of these limits on auditors' liability may violate the AICPA independence standards. Notwithstanding the potential applicability of auditor-independence standards, the limitation-of-liability provisions discussed in the advisory present safety-and-soundness concerns for all financial institution audits.

54. For banks, see section 36 of the FDI Act (12 USC 1831m) and part 363 of the FDIC's regulations (12 CFR 363).

55. Public companies are companies subject to the reporting requirements of the Securities Exchange Act of 1934.

56. See part 363 of the FDIC's regulation (12 CFR 363), *Appendix A—Guidelines and Interpretations,* Guideline 14, *"Role of the Independent Public Accountant-Independence."*

57. In contrast to the SEC's position, AICPA Ethics Ruling 94 (ET, section 191.188–189) currently concludes that indemnification for "knowing misrepresentations by management" does *not* impair independence.

Alternative Dispute-Resolution Agreements and Jury-Trial Waivers

The agencies observed that a review of the engagement letters of some financial institutions revealed that they had agreed to submit disputes over external audit services to mandatory and binding alternative dispute resolution, binding arbitration, or other binding nonjudicial dispute-resolution processes (collectively, *mandatory ADR*) or to waive the right to a jury trial. By agreeing in advance to submit disputes to mandatory ADR, financial institutions may waive the right to full discovery, limit appellate review, or limit or waive other rights and protections available in ordinary litigation proceedings.

Mandatory ADR procedures and jury-trial waivers may be efficient and cost-effective tools for resolving disputes in some cases. Accordingly, the agencies believe that mandatory ADR or waiver of jury-trial provisions in external audit engagement letters do not present safety-and-soundness concerns, provided that the engagement letters do not also incorporate limitation-of-liability provisions. Institutions are encouraged to carefully review mandatory ADR and jury-trial provisions in engagement letters, as well as review any agreements regarding rules of procedure, and to fully comprehend the ramifications of any agreement to waive any available remedies. Financial institutions should ensure that any mandatory ADR provisions in audit engagement letters are commercially reasonable and—

- apply equally to all parties,
- provide a fair process (for example, neutral decision makers and appropriate hearing procedures), and
- are not imposed in a coercive manner.

The Advisory's Conclusion

Financial institutions' boards of directors, audit committees, and management should not enter into any agreement that incorporates limitation-of-liability provisions with respect to audits. In addition, financial institutions should document their business rationale for agreeing to any other provisions that limit their legal rights.

The inclusion of limitation-of-liability provisions in external audit engagement letters and other agreements that are inconsistent with the advisory will generally be considered an unsafe and unsound practice. Examiners will consider the policies, processes, and personnel surrounding a financial institution's external auditing program in determining whether (1) the engagement letter covering external auditing activities raises any safety-and-soundness concerns and (2) the external auditor maintains appropriate independence regarding relationships with the financial institution under relevant professional standards. The agencies may take appropriate supervisory action if unsafe and unsound limitation-of-liability provisions are included in external audit engagement letters or other agreements related to audits that are executed (accepted or agreed to by the financial institution).

CERTIFIED PUBLIC ACCOUNTANTS

This section discusses the standards for competence and independence of certified public accountants (CPAs) as well as the standards required in connection with their audits.

Standards of Conduct

The Code of Professional Ethics for CPAs who are members of the American Institute of Certified Public Accountants (AICPA) requires that audits be performed according to generally accepted auditing standards (GAAS). GAAS, as distinct from generally accepted accounting principles, or GAAP, are concerned with the auditor's professional qualifications, the judgment the auditor exercises in the performance of an audit, and the quality of the audit procedures.

On the other hand, GAAP represents all of the conventions, rules, and procedures that are necessary to define accepted accounting practices at a particular time. GAAP includes broad guidelines of general application and detailed practices and procedures that have been issued by the Financial Accounting Standards Board (FASB), the AICPA, the SEC, or other authoritative bodies that set accounting standards. Thus, GAAP provides guidance on financial-reporting and disclosure matters.

Generally Accepted Auditing Standards

GAAS are grouped into three categories: general standards, standards of field work, and standards of reporting.

The *general standards* require that the audit be performed by a person or persons having adequate technical training and proficiency; that independence in mental attitude be maintained; and that due professional care be exercised in the performance of the audit and the preparation of the report.

Standards of field work require that the work be adequately planned; assistants, if any, be properly supervised; a proper study and evaluation of existing internal controls be made for determining the audit scope and the audit procedures to be performed during the audit; and sufficient evidence be obtained to formulate an opinion regarding the financial statements under audit.

Standards of reporting require that the CPA state whether the financial statements are presented in accordance with GAAP. The application of GAAP in audited financial statements and reports must achieve the fundamental objectives of financial accounting, which are to provide reliable financial information about the economic resources and obligations of a business enterprise. In addition, the informative disclosures in the financial statements must follow GAAP, or the CPA must state otherwise in the report.

GAAS recognizes that management—not the CPA—has primary responsibility for the preparation of the financial statements and the presentations therein. The auditor's responsibility is to express an opinion on the financial statements. GAAS (or the audit requirements previously set forth) require that audits cover the following financial statements: balance sheet, income statement, statement of changes in stockholders' equity, and statement of cash flows.

GAAS require that CPAs plan and perform auditing procedures to obtain reasonable assurance that financial statements are free from material misstatement. Under GAAS, an audit includes examining on a test basis and should include evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial-statement presentation.

Independence

In the performance of their work, CPAs must be independent of those they serve. Traditionally, independence has been defined as the ability to act with integrity and objectivity. In accordance with the rule on independence included in the SEC's independence rules and the Code of Professional Ethics and related AICPA interpretations, the independence of a CPA is considered to be impaired if, during the period of his or her professional engagement, the CPA or his or her firm had any direct or material indirect financial interest in the enterprise or had any loan to or from the enterprise or any officer, director, or principal stockholder thereof. The latter prohibition does not apply to the following loans from a financial institution when made under normal lending procedures, terms, and requirements:

- automobile loans and leases collateralized by the automobile
- loans in the amount of the cash surrender value of a life insurance policy
- borrowings fully collateralized by cash deposits at the same financial institution (for example, passbook loans)
- credit cards and cash advances under lines of credit associated with checking accounts with aggregate unpaid balances of $5,000 or less

Such loans must, at all times, be kept current by the CPA as to all terms.

Other loans have been grandfathered by the AICPA under recent ethics interpretations. These other loans (mortgage loans, other secured loans, and loans not material to the AICPA member's net worth) must, at all times, be current as to all terms and shall not be renegotiated with the client financial institution after the latest of—

- January 1, 1992;
- the date that the financial institution first becomes a client;
- the date the loans are sold from a nonclient financial institution to the client financial institution; or
- the date of becoming a member in the AICPA.

The examiner may decide under certain circumstances to test the independence of the CPA through reviews of loan listings, contracts, stockholder listings, and other appropriate measures. Concerns about independence should be identified in the report of examination.

The SEC has also released guidance relating to the independence of auditors for public institutions. According to SEC Rule 101, the independence of an auditor would be impaired if financial, employment, or business relationships exist between auditors and audit clients, and if there are relationships between auditors and audit clients in which the auditors provide certain nonaudit services to their audit clients. Much of the language found in the SEC's independence rules is incorporated in the Interagency Policy Statement on the Internal Audit Function and Its Outsourcing.

EXTERNAL AUDIT REPORTS

The external auditor generates various types of reports and other documents. These reports typically include—

- the standard audit report, which is generally a one-page document;
- a "management letter" in which the auditor confidentially presents detailed findings and recommendations to management; and
- an attestation report in which the auditor attests to management's assertion of internal controls and procedures over financial reports (for public companies and institutions subject to section 36 of the FDI Act); and
- other reports from the auditor to regulators during the audit period.

The major types of standard audit reports will never have a heading or other statement in the report that identifies which type it is. Rather, the type of report is identified by certain terminology used in the text of the report. The major types of standard audit reports are described below.

The *unqualified report,* sometimes referred to as a *clean opinion,* states that the financial statements are "presented fairly" in conformity with GAAP and that the necessary audit work was done.

The *qualified report* may generally have the same language as the unqualified report but will use the phrase "except for" or some other qualification to indicate that some problem exists. The types of problems include a lack of sufficient evidential matter, restrictions on the scope of audit work, or departures from GAAP in the financial statements. This type of report is not necessarily negative but indicates that the examiner should ask additional questions of management.

An *adverse report* basically concludes that the financial statements are not presented fairly in conformity with GAAP. This type of report is rarely issued because auditors and management usually work out their differences in advance.

A *disclaimer* expresses no opinion on the financial statements. CPAs may issue a disclaimer when they have concluded that substantial doubt exists about the ability of the institution to continue as a going concern for a reasonable period of time. This disclaimer is intended to indicate that the CPA is not assuming any responsibility for these statements.

REVIEW OF THE EXTERNAL AUDITOR'S INDEPENDENCE AND AUDIT

Because of the professional and ethical standards of the public accounting profession, the Federal Reserve has concluded that the examiner should conduct an in-depth review of the competence and independence of the CPA only in unusual situations. One such situation would be a recent change in CPAs by a bank, particularly if the change was made after an audit had commenced.

Ordinarily, specific tests to determine independence are not necessary. However, there may be occasions when the examiner has sufficient reason to question the independence of a CPA or the quality of his or her work. For example, the examiner may discover that during the period of a CPA's professional engagement, which includes the period covered by the financial statements on which the CPA has expressed an opinion, the CPA or a member of his or her firm—

- had a direct financial interest in the bank;

- was connected with the bank in a capacity equivalent to that of a member of management or was a director of the bank;
- maintained, completely or in part, the books and records of the bank and did not perform audit tests with respect to such books and records; or
- had a prohibited loan from the bank (as discussed earlier).

In these and similar instances, the CPA would not have complied with professional standards.

The examiner should determine the scope of the CPA's examination by reviewing the most recent report issued by the CPA. If the audit is in progress or is planned to commence in the near future, the examiner should review any engagement letter to the bank from the CPA. The examiner also should obtain and review any adjusting journal entries suggested by the CPA at the conclusion of the examination. This should be done to determine whether such entries were the result of breakdowns in the internal control structure and procedures for financial reporting.

Under certain circumstances, a CPA may issue a qualified or adverse opinion or may disclaim an opinion on a bank's financial statements. In such circumstances, the examiner should first determine the reasons for the particular type of opinion issued. If the matters involved affect specific areas of the bank's operations, a review of the work performed by the CPA may help the examiner understand the problem that gave rise to this opinion. The examination procedures (section 1010.3) describes the steps the examiner should follow when conducting a review of the work performed by the CPA. (See the FFIEC interagency Policy Statement on the External Auditing Programs of Banks and Savings Associations (effective January 1, 2000) (SR-99-33)).

LIMITATIONS OF AUDITS AND AUDITED FINANCIAL STATEMENTS

Although auditing standards are designed to require the use of due care and objectivity, a properly designed and executed audit does not necessarily guarantee that all misstatements of amounts or omissions of disclosure in the financial statements have been detected. Moreover, a properly designed and executed audit does not guarantee that the auditor addressed FRB safety-and-soundness considerations. Examination personnel should be cognizant of the limitations inherent in an audit. The following examples illustrate some common limitations of audits:

- The auditor is not responsible for deciding whether an institution operates wisely. An unqualified audit report means that the transactions and balances are reported in accordance with GAAP. It does not mean that the transactions made business sense, that the associated risks are managed in a safe and sound manner, or that the balances can be recovered upon disposition or liquidation.
- The auditor's report concerning financial statements does not signify that underwriting standards, operating strategies, loan-monitoring systems, and workout procedures are adequate to mitigate losses if the environment changes. The auditor's report that financial statements fairly present the bank's financial position is based on the prevailing evidence and current environment, and it indicates that reported assets can be recovered in the normal course of business. In determining that reported assets can be recovered in the normal course of business, the auditor attempts to understand financial-reporting internal controls and can substitute other audit procedures when these controls are weak or nonexistent.
- The quality of management and how it manages risk are not considered in determining historical cost and its recoverability. Although certain assets and instruments are marked to market (for example, trading accounts), GAAP generally uses historical cost as the basis of presentation. Historical cost assumes that the entity is a going concern. The going-concern concept allows certain mark-to-market losses to be deferred because management believes the cost basis can be recovered during the remaining life of the asset.
- GAAP financial statements offer only limited disclosures of risks, uncertainties, and the other safety-and-soundness factors on which the institution's viability depends.
- Under GAAP, loan-loss reserves are provided for "probable losses" currently "inherent" (that is, anticipated future charge-offs are based on current repayment characteristics) in the portfolio. GAAP defines probable as the likelihood that a future event will occur, confirming the fact of the loss. Additionally, the amount of the loss must be reasonably estimable.

COMMUNICATION WITH EXTERNAL AUDITORS

GAAS requires that the external auditor can consider regulatory authorities as a source of competent evidential matter when conducting an audit of the financial statements of a banking organization. Accordingly, an external auditor may review communications from, and make inquiries of, the regulatory authorities.

Generally, the Federal Reserve encourages auditors to attend examination exit conferences upon completion of the examiner's field work or to attend other meetings concerning examination findings between supervisory examiners and an institution's management or board of directors (or a committee thereof). Banks should ensure that their external auditors are informed in a timely manner of scheduled exit conferences and other relevant meetings with examiners and of the FRB's policies regarding auditor attendance at such meetings.

When other conferences between examiners and management are scheduled (those that do not involve examination findings that are relevant to the scope of the external auditor's work), the institution should first obtain the approval of the appropriate Federal Reserve Bank personnel for the auditor to attend the meetings. The interagency policy statement of July 23, 1992, does not preclude the Federal Reserve from holding meetings with the management of banks without auditor attendance or from requiring that the auditor attend only certain portions of the meetings. (See SR-92-28.)

The 1992 interagency policy statement was issued to improve coordination and communication between external auditors and examiners. Examination personnel should provide banking organizations with advance notice of the starting date of the examination when appropriate, so management can inform external auditors in advance and facilitate the planning and scheduling of their audit work.

Some institutions prefer that audit work be completed at different times than examination work to reduce demands on their staff members and facilities. Other institutions prefer to have audit work and examination work performed during similar periods so the institution's operations are affected only at certain times during the year. By knowing when examinations are planned, institutions have the flexibility to schedule external audit work concurrent with, or separate from, examinations.

Meetings and Discussions Between External Auditors and Examiners

An external auditor may request a meeting with the FRB regulatory authorities involved in the supervision of the institution or its holding company during or after completion of examinations to inquire about supervisory matters relevant to the institution under audit. External auditors should provide an agenda in advance. The FRB regulatory authorities will generally request that management of the institution under audit be represented at the meeting. In this regard, examiners will generally only discuss with an auditor examination findings that have been presented to bank management.

In certain cases, external auditors may wish to discuss with examiners matters relevant to the institution without bank management representation. External auditors may request such confidential meetings with the FRB regulatory authorities, who may also request such meetings with the external auditor.

Information Required to Be Made Available to External Auditors

Section 931 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) and section 112 of FDICIA (12 USC 1811) pertain to depository institutions insured by the FDIC that have engaged the services of an external auditor to audit the banking organization within the past two years. FIRREA and FDICIA require banks to provide the auditor with copies of the most recent Report of Condition (Call Report), report of examination, and pertinent correspondence or reports received from its regulator. This information is to be provided to the external auditor by the bank under audit, not by the FRB. In addition, banking organizations must provide the independent auditor with—

- a copy of any supervisory memorandum of understanding or written agreement between a federal or state banking agency and the bank put into effect during the period covered by the audit, and

- a report of any formal action taken by a federal or state banking agency during such period, or any civil money penalty assessed with respect to the bank or any banking organization–affiliated party.

Regulatory personnel should ascertain if the banking organization is in compliance with the requirements of section 931 of FIRREA (12 USC 1817(a)) and section 112 of FDICIA and should report instances of noncompliance in the report of examination.

Confidentiality of Supervisory Information

While the policies of the FRB regulatory authorities permit external auditors to have access to the information described above, institutions and their auditors are reminded that information contained in examination reports, inspection reports, and supervisory discussions—including any summaries or quotations—is confidential supervisory information and must not be disclosed to any party without the written permission of the FRB. Unauthorized disclosure of confidential supervisory information may lead to civil and criminal actions and fines and other penalties.

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

- Management and Internal Control Evaluation
- Internal and External Audit Evaluation

The information in the first part of this section is largely reprinted from a publication of the Bank Administration Institute (BAI), entitled "Statement of Principle and Standards for Internal Auditing in the Banking Industry." The second part of this section reproduces appendixes A and B from the February 9, 2006, Interagency Advisory on the Unsafe and Unsound Use of Limitation of Liability Provisions in External Audit Engagement Letters.

A STATEMENT OF PRINCIPLE CONCERNING INTERNAL AUDITING IN THE BANKING INDUSTRY

Internal auditing is that management function which independently evaluates the adequacy, effectiveness and efficiency of the systems of control within an organization and the quality of ongoing operations.

The systems of control comprise the plan of organization and all methods and measures designed to:

- Provide reasonable assurance that assets are safeguarded, information (financial and other) is timely and reliable, and errors and irregularities are discovered and corrected promptly.
- Promote operational efficiency.
- Encourage compliance with managerial policies, laws, regulations, and sound fiduciary principles.

Ongoing operations comprise all activities involved in the conduct of the organization's business.

The internal auditor is accountable to the board of directors and executive management. This accountability precludes the auditor from organizational relationships that may conflict with the need for independence.

STANDARDS OF INTERNAL AUDITING IN THE BANKING INDUSTRY

Organization Standards

1. The organization shall have an internal audit function responsible for evaluating the adequacy, effectiveness and efficiency of its systems of control and the quality of ongoing operations.
2. The organization shall maintain an environment within which the auditor has the freedom to act.
3. The organization shall allocate sufficient resources to the audit function to enable it to conform to the standards of internal auditing.
4. The organization shall require management to respond formally to adverse audit findings and to take appropriate corrective action.
5. The organization's systems of control shall include measurement of audit effectiveness and efficiency.

Personal Standards

1. An internal auditor shall have adequate technical training and proficiency.
2. An internal auditor shall maintain a sufficiently independent state of mind to clearly demonstrate objectivity in matters affecting audit conclusions.
3. An internal auditor shall respect the confidentiality of information acquired while performing the audit function.
4. An internal auditor shall only engage in activities that do not conflict with the interests of the organization.
5. An internal auditor shall adhere to conduct that enhances the professional stature of internal auditing.
6. An internal auditor shall exercise due professional care in the performance of all duties and in the fulfillment of all responsibilities.

Performance Standards

1. The internal auditor shall prepare a formal audit plan that covers all significant organizational activities over an appropriate cycle of time.
2. The audit plan shall include an evaluation of controls within new systems and significant modifications to existing systems before they become operational.
3. Audit procedures shall provide sufficient and competent evidential matter to support conclusions regarding the adequacy, effectiveness and efficiency of the systems of control and the quality of ongoing operations.
4. The organization of the audit function and related administrative practice shall provide for the proper supervision of persons performing audits and for the proper review of work performed.

Communication Standards

1. The auditor shall prepare a formal report on the scope and results of each audit performed.
2. Each audit report shall contain an opinion on the adequacy, effectiveness and efficiency of the systems of control and the quality of ongoing operations; the degree of compliance with previously evaluated systems of control; or an explanation of why an opinion cannot be expressed. When an adverse opinion is expressed, the report shall contain a statement about the exposures that may exist in the absence of corrective action.
3. The auditor shall communicate audit findings in a timely manner to the managers responsible for corrective action.
4. At least once each year the auditor shall make a summary report of audit activities to the board of directors and executive management. The report shall include an opinion on the overall condition of the organization's controls and operations.

COMMENTARY

The following comments are presented in order to promote the acceptance of the "Statement of Principle and Standards for Internal Auditing in the Banking Industry," to provide a context for the application of its concepts and to enhance the understanding of internal auditing. It is intended that the statement and the commentary will serve as a basis for the continuing advancement of the profession's influence and service.

Internal Auditing as a Discipline

Internal auditing is developing a broader perspective by recognizing that all operations are properly subject to control and within the scope of auditing. The internal auditor's concern for control should extend beyond accounting matters. This broader concept better serves the board of directors and executive management to whom the internal auditor is accountable. Bank Administration Institute believes the systems of control and ongoing operations, as defined herein, provide a preferred perspective for discussing internal auditing within the framework of the auditing discipline taken as a whole.

Concepts of Control

The systems of control exist to assure the achievement of intended results, to promote operating efficiency and to encourage compliance with policies and other established constraints. Although internal auditors have a definite interest in verifying the results of business activity, their primary concern must be the continuing effectiveness of the systems of control that influence business results. The important qualities that must be evaluated are adequacy, effectiveness and efficiency.

In evaluating adequacy, the auditor analyzes systems to determine that they include design features proper to the circumstances and reasonably sufficient to effect control. The evaluation of adequacy begins with the comparison of "what should be" to "what is." Initial audits and audits of proposed procedures or organization structures focus primarily on the adequacy of control.

In evaluating effectiveness, the auditor measures the degree of compliance with control features and the extent to which compliance serves the intended purposes. The question that must be answered is: "Do the controls work?"

In evaluating efficiency, the auditor judges the practicality of controls in terms of their cost relative to their intended benefit. It is not intended that the auditor should evaluate ad-

equacy or effectiveness in absolute terms, nor is it intended that the auditor judge efficiency in absolute terms. An internal auditor's evaluation of efficiency is restricted to the controls themselves and does not extend to the measures of operating performance associated with the functioning of such controls. In judging efficiency, the internal auditor must conclude whether the benefits provided by the controls exceed their cost.

The systems of control and not the audit function:

- Provide reasonable assurance that assets are safeguarded, information (financial and other) is timely and reliable, and errors and irregularities are discovered and promptly corrected.
- Promote operational efficiency.
- Encourage adherence to managerial policies, laws, regulations and sound fiduciary principles.

Those members of management who are responsible for policy implementation are also responsible for the design and the maintenance of the systems of control. Internal auditors are responsible for that management function which independently evaluates the adequacy, effectiveness and efficiency of the systems of control. Internal auditors should make sure that those who rely on their opinions understand that no practical system can guarantee the quality of future performance.

Controls act as a positive force to facilitate successful operations as well as a negative one that restricts activities. Accordingly, the auditor should evaluate control systems in terms of the incentives they provide as well as the sanctions.

Safeguarding assets relates to physical, legal and all other protective means by which the organization assures the full realization of its resources.

All information should be subject to the systems of control. Timely information is that which anticipates a decision need and is available to the persons who will use it when they need it. Reliable information provides a sound basis for decision because of the authenticity of its source, the manner in which it is recorded and the form and content of its presentation.

The systems of control must detect and correct errors and irregularities when preventive controls fail. Sound systems of control contain safeguards that will counteract failures in other controls.

The systems of control should promote operational efficiency. The features of control systems that promote operational efficiency include the processes used to select and train personnel, establish procedures, set performance requirements, measure results and provide incentives.

Managerial policies, laws, regulations and sound fiduciary principles establish bounds within which the organization can conduct its business. The features of the control system that encourage compliance with these requirements include the separation of duties, the employment of persons likely to comply, the establishment of authority limits and the communication of expected conduct.

Ongoing Operations

Management must evaluate the quality of operations based on information provided by the control systems. Adequate control systems produce sufficient information to reliably appraise operations. To confirm that the control systems are adequate and effective, the internal auditor should independently evaluate the quality of ongoing operations. Only ongoing operations have future significance.

Internal auditors should express their opinion on whether the quality of ongoing operations is satisfactory or unsatisfactory. Satisfactory operations are those which, in the opinion of the auditor, require no extraordinary intervention by executive management or the directors. Conversely, unsatisfactory operations require extraordinary intervention before appropriate remedial action is likely to occur. A qualified opinion may be expressed by citing specific exceptions to satisfactory operations. Auditors may assess the quality of operations more precisely and report on grades of quality, provided the grades are clearly understood by management.

Circumstances may preclude the auditor from forming an opinion on the quality of ongoing operations. This, by itself, is significant because the information provided by the control systems should be adequate for the evaluation of ongoing operations.

Accountability

Accountability refers to the measures of effective audit performance. The organization standards of this statement define the conditions necessary to hold the auditor accountable for the other standards.

Only the board of directors can protect the auditor's need for independence; consequently, the board should be the final judge of the auditor's performance. The fact that the process of measurement may be done through an audit committee does not alter the auditor's ultimate accountability to the board.

Both the auditor and executive management have received a delegation of authority from the board: management to design and maintain systems of control; the auditor to evaluate these systems of control. Because the evaluation process exists to serve the design and maintenance responsibility, the auditor must also be accountable to executive management. This accountability, however, does not create the usual corollary right of the executive to directly apply sanctions or to otherwise restrict the auditor's functional independence. Such action, if necessary, must be decided by the board.

The auditor should be mindful that the audit function serves many users. The auditor has an obligation, if not accountability, to those users. The auditor's personal relationship with others should be characterized by integrity, open communication and mutual respect. User satisfaction should be an important consideration in the board's evaluation of audit performance.

Independence is a matter of personal quality rather than of rules. The auditor's relationships, as indicated by the plan of organization and by the way in which the work is conducted, must always be such that a presumption of independence logically follows in the mind of the observer.

Organization Standards

A banking organization can best evidence its support and commitment to the professional standards of internal auditing by formally adopting these standards.

The organization standards are prerequisites to the personal, performance and communication standards. The simply state that an internal auditor cannot be accountable for adherence to the other standards without the necessary resources and support of the organization.

Many banks cannot afford the services of a competent and independent internal auditor. It should be clearly understood that those banks are not in compliance with these standards. Their directors and executive management, therefore, bear the burden of providing additional supervision to assure the adequacy, effectiveness and efficiency of the systems of control and the quality of ongoing operations.

The organization shall provide and maintain an environment within which the internal auditor has the freedom to act. Persons whose duties and responsibilities are subject to audit cannot have the authority to regulate the scope of audit work nor the procedures considered necessary by the auditors. The auditor's responsibility to independently evaluate the systems of control must carry with it the authority to set the scope and choose the means of examination.

Budgeting should be based on a complete plan of audit that demonstrates fulfillment of the organization's audit needs and adherence to the standards of internal auditing. In committing resources to the internal audit function, the organization should expect the auditor to properly support requested allocations through the established budget process.

The audit process is not complete until the auditor is satisfied that audit findings have received appropriate attention. By requiring management to respond formally to audit findings, the organization contributes to the effectiveness of the audit function and increases the likelihood that the findings will receive appropriate attention.

The organization should measure the performance of its internal audit function in relation to the timeliness, efficiency and the quality of its work. Timeliness is indicated by scheduling the work in recognition of risk assessments and by the prompt issuance of reports. Efficiency is indicated by completing the work within the time budgeted. An efficient internal audit program also minimizes the time required by examiners and public accountants without affecting adequate coverage. Formal work programs, workpapers and the form and content of reports evidence the quality of an audit function. The organization should consider using the opinions formed by bank examiners, certified public accountants and other professional auditors to assist in this performance evaluation. Smaller banks may find the services offered by their correspondents include such evaluations.

Personal Standards

Personal standards relate to the qualifications of auditors, the quality of audit practice and the rules of professional conduct. They concern all persons who apply audit procedures under a delegation of authority from the board to support conclusions regarding the systems of control. Personal standards are prerequisites to performance and communication standards.

All persons engaged in the practice of internal auditing shall have the technical training and proficiency necessary to conduct their audit duties in accordance with these standards. Technical training and proficiency are separate requirements. Technical training relates to education; proficiency relates to the skill and judgment acquired through experience.

The qualified internal auditor will have successfully completed a course of study and training in disciplines having audit significance and will understand their application to banking. These disciplines include the principles of accounting, auditing, economics, finance, operations analysis, management, statistics, commercial law and computer science.

Experience is gained by working under the close supervision and review of an experienced professional. This relationship should make the job itself a vehicle for seasoning and refining the technical training acquired through formal education. On-the-job training should be carefully planned and organized. Those responsible for managing the audit function should define the elements of knowledge and judgment that may be gained from experience and establish a way to measure the resulting proficiency.

Proficiency is demonstrated by the proper exercise of professional judgment. It is difficult for users of professional services to accurately assess proficiency. Therefore, recognized professions, including internal auditing, provide certification programs for their practitioners. Each person engaged in the internal audit function can demonstrate proficiency by earning a professional designation such as chartered bank auditor, certified internal auditor or certified public accountant. The last two designations, however, require successful banking or related experience to demonstrate a practical knowledge of the industry.

The modern business environment demands that an internal auditor maintain proficiency by active participation in programs of continuing education and professional association.

There is no concept more important to internal auditing than independence. The essence of independence is intellectual honesty informing conclusions and expressing opinions. Conclusions must be reached fairly without bias or the propensity to prejudge circumstances. Opinions must be expressed forthrightly despite the conflicts that may arise. Although the appearance of independence relies on a plan of organization that grants the auditor freedom from conflicting accountabilities, the actual attainment of independence depends solely on the individual. The concept of independence is most fundamental to the definition and practice of auditing.

Independence is not isolation. Auditors should not allow their need for independence to inhibit the contacts and rapport necessary for a fully effective audit function.

Banking organizations properly require all employees to honor the confidentiality of financial and other information obtained during their employment. This requirement is all the more important for internal auditors because of the nature and scope of their work. Confidentiality also applies to the judicious use of information within the organization.

An internal auditor should not accept employment or participate in activities that compete or otherwise oppose the lawful objectives of the organization. Loyalty reflects integrity and credibility. Relationships which may, even by implication, raise doubt concerning the auditor's loyalty to the bank therefore must be avoided.

Internal auditors develop professional recognition by supporting and participating in associations organized to serve their common needs. Each internal auditor is also obligated to maintain proficiency and awareness through self-education.

Due professional care imposes an ethical obligation on all auditors to demonstrate competency. Due care acts as a safeguard against negligence and oversight. Due professional care applies to the administrative practices that bear on the quality of audit results as well as to the use of audit procedures that provide sufficient competent evidence.

Due professional care is a subjective standard based on reasonableness. The duty of due professional care requires the auditor to know the extent of reliance that others within the organization place on audit results. When such reliance is unrealistic or misunderstood, the auditor

should resolve the misunderstanding and temper unrealistic expectations.

The organization should require the presentation of audit findings in a manner that convinces management that the auditor exercised due professional care.

Performance Standards

The audit plan should be written and presented in a form that is suitable for critical review by audit committees, certified public accountants, regulatory examiners and others who must evaluate the adequacy of audit coverage.

An audit plan is based on a catalog of examinations that includes all significant activities of the organization classified by logical units for work scheduling. For example, demand deposit bookkeeping functions may be classified as three separate audits: overdraft control practices, confirmation of balances and bookkeeping operations.

The frequency of audit should be determined by reference to factors affecting risk, management information, customer satisfaction and the need to create an awareness of audit presence. Risk assessment involves audit judgment regarding how often and to what extent the systems of control must be evaluated.

In mature audit operations, the problem of balancing audit objectives with audit resources has usally been solved. Risk assessment in the context of audit planning does not normally change in the near range. The audit plan for each cycle does not prescribe a detailed listing of tests and procedures to be applied. These tactical steps are to be found in the work program.

The audit plan, which usually represents work contemplated for the current year, should present the information necessary to schedule and assign the work. It should cover resources requirements, administrative goals and objectives and the estimated costs of audit. Resource plans identify the number of persons needed, schedule their time (including such non-audit time as administration, vacation, lost days, staff training) and specify the level of ability. Administrative goals and objectives should reflect the audit implications of conditions that influence the organization. Audit costs should be identified in sufficient detail to encourage the audit manager to justify their cost and impact on the organization.

While cost justifying the audit plan, the auditor should recognize that the organization's cost of control includes its cost of auditing. In certain areas, efficiencies may best be achieved by strengthening the control systems as an alternative to audit coverage.

The audit plan shall include an evaluation of the adequacy of controls within new systems and significant modifications to existing systems before they become operational. This evaluation should include the controls designed into the conversion plan. Significant modifications are those that affect controls to an extent that audit concern is created regarding the organization's resulting exposure to loss.

The second performance standard concerns the timing of audit but not its scope. Identifying significant changes and establishing audit procedures is a matter of individual audit judgment. Modern complex systems are expensive to develop and maintain. Building adequate controls within the original design is usually less costly than adding them after the system is operational. The cost of evaluation, however, is usually no greater before implementation than after.

The reliability of audit results depends on the character of supporting evidence. Audit procedures should be selected and applied in a way that assures such evidence is sufficient and competent.

The term "sufficient" as used here means that enough evidence is assembled to assure that audit conclusions are well founded. The internal auditor's determination of what constitutes enough evidence is a matter of professional judgment relative to the controls and operations under evaluation. Frequently, sufficiency can be demonstrated by the application of statistical sampling techniques.

The term "competent" means relevant and valid. Competent evidence has the requisite ability to convince. Both the substance and the interrelationship of evidence demonstrate competence. Whereas sufficient is a quantitative concept, competent is a qualitative one.

Competency for audit purposes depends on the procedures used to obtain evidence. Direct knowledge, such as obtained by observation or inspection, is more reliable than indirect knowledge, such as obtained by confirmation and inquiry. Obtaining the most competent evidence, however, is not always feasible. Selecting and applying those procedures that collectively pro-

duce the most competent evidence under the circumstances demonstrates audits proficiency.

Audit work should be organized so that the objectives at each level of detail are clearly defined. Each phase of the work as well as the contribution of each person should be viewed by a superior. Audit management should review the audit programs, questionnaires and other planning features for completeness, applicability and efficiency. The reviewer should be satisfied that those who perform field work understand the systems under examination and the audit procedures that have been selected for application.

The auditor in charge of each assignment should perform a detailed review of the work as it is completed. No work should be accepted unless it complies with the standard of evidence. Audit management should conduct a comprehensive final review of the workpapers to determine that proper procedures were applied, sufficient evidence was assembled and all exceptions were properly evaluated in terms of their control significance. Audit management should also make interim field reviews.

Reviews must be documented. All auditors should appreciate the importance of the review process and perform their work in a manner that facilitates review. Review serves as an educational process as well as a control. Directors of banks employing only one auditor should supervise the auditor's work in a manner that provides a check on audit quality.

Communication Standards

The auditor has a responsibility to report the results of all audit work performed. Some auditors prefer to report only significant exceptions; however, this practice reinforces a negative view of the audit function. The auditor's responsibility to evaluate control systems and ongoing operations carries with it an obligation to report the results of that evaluation. Without a report, management does not have positive assurance that auditing is meeting its commitments. Consequently, management can only assume that adequate coverage is maintained and that the systems of control are functioning adequately, effectively and efficiently. By implication, audit reporting only on an exception basis extends the auditor's responsibility beyond what the actual work can support and causes misunderstanding.

Requiring auditors to express an opinion on the adequacy, effectiveness and efficiency of the systems of control and the quality of ongoing operations enables the board of directors, management and other interested parties to better judge the reliability of the control systems and ongoing operations. This service is a natural and logical part of the internal auditor's accountability.

Expressing an opinion imposes a serious obligation on the auditor. The requirement of due professional care extends to both the opinion and the commentary supporting it. Clear identification of the systems of control audited is the key to a meaningful opinion.

Each auditor should develop standard language for rendering an opinion. Standardization of language minimizes misunderstanding and promotes recognition of circumstances that require responsive action.

It is suggested that auditors develop their opinion statement along the following lines:

"In our opinion (the audit subject's) operating and accounting procedures include those practices usually necessary to provide adequate and efficient control. Also in our opinion, the degree of compliance with such procedures provided effective control during the (period of audit). We found the quality of ongoing operations satisfactory."

This opinion assumes the auditor has reviewed the systems of control before they became operational and is satisfied that they include design features proper to the circumstances and reasonably sufficient to effect control. The second sentence of the opinion addresses the degree of compliance with control features previously found adequate and efficient. Audits of operations that are subject to a common control system such as a typical branch bank audit need not include a review of the system each time a unit audit is performed. The auditor, however, should be satisfied that all modifications to the existing system that significantly affect control have been evaluated.

Auditors occasionally form adverse conclusions concerning the adequacy, effectiveness or efficiency of the systems of control or the quality of ongoing operations. In these cases, they should qualify their opinion and identify exposures that may exist in the absence of corrective action. Risk measures the degree to which exposures are uncontrolled. The applica-

ble equation is: Exposure minus control equals risk. A calculated risk is taken only when the exposure is fully identified and the implications of the lack of control are understood. To make an adverse opinion clear and meaningful, therefore, the auditor must identify relevant exposures and explain their significance.

Every audit report should identify the area audited and disclose all matters the auditor believes require responsive action by the recipient. Auditors should clearly distinguish between those matters to which they take exception and those that are reported for other reasons. The degree of detail reported is largely a matter of judgment, influenced greatly by the preferences of management. Some managements prefer to have all audit findings reported no matter how minor. Others prefer only a general description of significant findings. Auditors must bear in mind that their ultimate accountability demands that findings of major significance be brought to the attention of executive management and the board of directors.

The standards do not require the auditor to recommend corrective action. In practice, however, auditors find that many managements expect suggestions for corrective action, particularly when the technincal aspects of controls are involved. By suggesting corrective action, the auditor demonstrates a positive approach to the organization's problems. In making suggestions, auditors should recognize that their recommendations may not be the only means of achieving the control purpose intended. The focus of concern should be the control purpose and not the particular means selected from a range of acceptable choices.

A draft of each audit report should be made available to the manager of those operations under examination. Findings should be discussed with the manager before final issuance of the report. Any revisions should be similarly reviewed. The final report must clearly present audit findings and avoid language that may imply a meaning inconsistent with the supporting evidence. A review and a discussion of the draft assure this result.

Auditors must establish the facts of their findings but do not have to obtain complete management acceptance of their comments before issuing a report. Auditors should be prepared for occasional conflict and disagreement.

The ease with which auditors can retrieve information, support fact and amplify findings validates the adequacy and the quality of audit evidence. The extent to which auditors gain acceptance of their comments ultimately measures the effectiveness of internal auditing's contribution to the organization.

The timeliness with which audit findings are reported is very important and often critical for effective response. When timeliness is critical, the auditor should communicate findings promptly and not await the preparation of a formal report. Findings should be communicated to the manager whose operation is directly affected.

The extent and frequency of audit reports required by the board of directors varies with the organization. At least annually, however, the auditor shall formally report to the board of directors and executive management. The board of directors and executive management are entitled to a report that measures audit performance against plan and provides information normally required to establish accountability. The auditor should use this opportunity to promote an understanding of the audit function and how it serves the organization.

In the summary report, the auditor should express an opinion on the overall condition of the organization's controls and ongoing operations. The report should present all known control problems of significance as well as an evaluation of corrective action taken. Although the report is formal, it should be presented personally to ensure proper interpretation and to provide the benefit that flows from the exchange of information and concerns.

Fraud and the Auditor's Responsibility

The auditor is charged with understanding the purposes of the business, the control practices usually necessary to achieve them, and the type of evidence that indicates they will continue to be achieved. The following questions are prerequisite to evaluating the systems of control: What is the purpose of the system? How is it controlled? What can go wrong?

Audit proficiency includes the ability to evaluate fraud exposures. Sufficient information is available in the literature on auditing concerning how frauds may be committed in banking. The auditor should be familiar with that literature.

The systems of control and not the internal audit function provide the primary assurance

against fraud. Internal auditors, however, must evaluate the capability of the systems to achieve that end. When in doubt, the auditor should consider applying additional procedures to determine if fraud has actually occurred.

In fixing the internal auditor's responsibility for detecting fraud, it should be recognized that the internal auditor cannot be responsible for detecting irregular transactions for which there is no record, e.g., an unrecorded receipt of cash from a source for which there is no evidence of accountability; an isolated transaction that does not recur, e.g., a single fraudulent loan; or irregularities that are well concealed by collusion. However, in the usual course of the audit cycle, the internal auditor should detect irregularities that significantly affect the financial statements, repeatedly follow a suspicious pattern of concurrence, or those that can be detected by a reasonable audit sampling. Internal auditors must also accept responsibility for those irregularities that result from their failure to report known weaknesses in the systems of control.

In judging the preventive capacity of the control systems and the internal auditor's responsibility, the principle of relative risk should not be ignored, namely, costs must be balanced against intended benefit.

CONCLUSION

Professional internal auditors can contribute a wealth of information to their organizations over and above the assurance they provide by evaluating the quality of control systems and ongoing operations. The word, "audit," comes from the Latin word, *audire*, meaning to hear. Internal auditors should be good listeners and observers. They should demonstrate an in-depth understanding of the strengths and weaknesses of the organization, the accomplishments and current problems of its departments, the quality of its services, the pride and concerns of its people and the efficiencies and diseconomies of its operations. In turn, executives and directors should listen to professional internal auditors and capitalize on their observations.

EXAMPLES OF UNSAFE AND UNSOUND LIMITATION-OF-LIABILITY PROVISIONS

The following information was contained in appendix A of the February 9, 2006, interagency advisory.

Presented below are some of the types of limitation-of-liability provisions (with an illustrative example of each type) that the agencies observed in financial institutions' external audit engagement letters. The inclusion in external audit engagement letters or agreements related to audits of any of the illustrative provisions (which do not represent an all-inclusive list) or any other language that would produce similar effects is considered an unsafe and unsound practice.

1. "Release from Liability for Auditor Negligence" Provision

In this type of provision, the financial institution agrees *not* to hold the audit firm liable for *any* damages, *except* to the extent determined to have resulted from willful misconduct or fraudulent behavior by the audit firm.

Example: In no event shall [the audit firm] be liable to the Financial Institution, whether a claim be in tort, contract or otherwise, for any consequential, indirect, lost profit, or similar damages relating to [the audit firm's] services provided under this engagement letter, except to the extent finally determined to have resulted from the willful misconduct or fraudulent behavior of [the audit firm] relating to such services.

2. "No Damages" Provision

In this type of provision, the financial institution agrees that *in no event* will the external audit firm's liability include responsibility for any compensatory (incidental or consequential) damages claimed by the financial institution.

Example: In no event will [the audit firm's] liability under the terms of this Agreement include responsibility for any claimed incidental or consequential damages.

3. "Limitation of Period to File Claim" Provision

In this type of provision, the financial institution agrees that *no* claim will be asserted after a fixed period of time that is shorter than the applicable statute of limitations, effectively agreeing to limit the financial institution's rights in filing a claim.

Example: It is agreed by the Financial Institution and [the audit firm] or any successors in interest that no claim arising out of services rendered pursuant to this agreement by, or on behalf of, the Financial Institution shall be asserted more than two years after the date of the last audit report issued by [the audit firm].

4. "Losses Occurring During Periods Audited" Provision

In this type of provision, the financial institution agrees that the external audit firm's liability will be limited to any losses occurring during periods covered by the external audit, and will *not* include any losses occurring in later periods for which the external audit firm is not engaged. This provision may not only preclude the collection of consequential damages for harm in later years, but could preclude any recovery at all. It appears that no claim of liability could be brought against the external audit firm until the external audit report is actually delivered. Under such a clause, any claim for liability thereafter might be precluded because the losses did not occur during the period covered by the external audit. In other words, it might limit the external audit firm's liability to a period before there could be any liability. Read more broadly, the external audit firm might be liable for losses that arise in subsequent years only if the firm continues to be engaged to audit the client's financial statements in those years.

Example: In the event the Financial Institution is dissatisfied with [the audit firm's] services, it is understood that [the audit firm's] liability, if any, arising from this engagement will be limited to any losses occurring during the periods covered by [the audit firm's] audit, and shall not include any losses occurring in later periods for which [the audit firm] is not engaged as auditors.

5. "No Assignment or Transfer" Provision

In this type of provision, the financial institution agrees that it will not assign or transfer any claim against the external audit firm to another party. This provision could limit the ability of another party to pursue a claim against the external auditor in a sale or merger of the financial institution, in a sale of certain assets or a line of business of the financial institution, or in a supervisory merger or receivership of the financial institution. This provision may also prevent the financial institution from subrogating a claim against its external auditor to the financial institution's insurer under its directors' and officers' liability or other insurance coverage.

Example: The Financial Institution agrees that it will not, directly or indirectly, agree to assign or transfer any claim against [the audit firm] arising out of this engagement to anyone.

6. "Knowing Misrepresentations by Management" Provision

In this type of provision, the financial institution releases and indemnifies the external audit firm from any claims, liabilities, and costs attributable to any knowing misrepresentation by management.

Example: Because of the importance of oral and written management representations to an effective audit, the Financial Institution releases and indemnifies [the audit firm] and its personnel from any and all claims, liabilities, costs, and expenses attributable to any knowing misrepresentation by management.

7. "Indemnification for Management Negligence" Provision

In this type of provision, the financial institution agrees to protect the external auditor from third-party claims arising from the external audit firm's failure to discover negligent conduct by management. It would also reinforce the defense of contributory negligence in cases in which the financial institution brings an action against its external auditor. In either case, the contractual defense would insulate the external audit firm

from claims for damages even if the reason the external auditor failed to discover the negligent conduct was a failure to conduct the external audit in accordance with generally accepted auditing standards or other applicable professional standards.

Example: The Financial Institution shall indemnify, hold harmless and defend [the audit firm] and its authorized agents, partners and employees from and against any and all claims, damages, demands, actions, costs and charges arising out of, or by reason of, the Financial Institution's negligent acts or failure to act hereunder.

8. "Damages Not to Exceed Fees Paid" Provision

In this type of provision, the financial institution agrees to limit the external auditor's liability to the amount of audit fees the financial institution paid the external auditor, regardless of the extent of damages. This may result in a substantial unrecoverable loss or cost to the financial institution.

Example: [The audit firm] shall not be liable for any claim for damages arising out of or in connection with any services provided herein to the Financial Institution in an amount greater than the amount of fees actually paid to [the audit firm] with respect to the services directly relating to and forming the basis of such claim.[1]

FREQUENTLY ASKED QUESTIONS ON THE APPLICATION OF THE SEC's AUDITOR-INDEPENDENCE RULES

The following information is contained in appendix B of the February 9, 2006, interagency advisory.

Question[2]

Inquiry was made as to whether an accountant who certifies financial statements included in a registration statement or annual report filed with the commission under the Securities Act or the Exchange Act would be considered independent if he had entered into an indemnity agreement with the registrant. In the particular illustration cited, the board of directors of the registrant formally approved the filing of a registration statement with the commission and agreed to indemnify and save harmless each and every accountant who certified any part of such statement "from any and all losses, claims, damages or liabilities arising out of such act or acts to which they or any of them may become subject under the Securities Act, as amended, or at 'common law,' other than for their willful misstatements or omissions."

Answer

When an accountant and his client, directly or through an affiliate, have entered into an agreement of indemnity which seeks to assure to the accountant immunity from liability for his own negligent acts, whether of omission or commission, one of the major stimuli to objective and unbiased consideration of the problems encountered in a particular engagement is removed or greatly weakened. Such condition must frequently induce a departure from the standards of objectivity and impartiality which the concept of independence implies. In such difficult matters, for example, as the determination of the scope of audit necessary, existence of such an agreement may easily lead to the use of less extensive or thorough procedures than would otherwise be followed. In other cases it may result in a failure to appraise with professional acumen the information disclosed by the examination. *Consequently, the accountant cannot be recognized as independent for the purpose of certifying the financial statements of the corporation.*

Question

Has there been any change in the commission's long-standing view (Financial Reporting

1. The agencies also observed a similar provision that limited damages to a predetermined amount not related to fees paid.

2. The subtitles in this section have been revised for this manual.

Policies—Section 600—602.02.f.i., "Indemnification by Client") that when an accountant enters into an indemnity agreement with the registrant, his or her independence would come into question?

Answer

No. When an accountant and his or her client, directly or through an affiliate, enter into an agreement of indemnity that seeks to provide the accountant immunity from liability for his or her own negligent acts, whether of omission or commission, the *accountant is not independent.* Further, including in engagement letters a clause that a registrant would release, indemnify or hold harmless from any liability and costs resulting from *knowing misrepresentations by management would also impair the firm's independence.*[3]

3. U.S. Securities and Exchange Commission; Office of the Chief Accountant: Application of the Commission's Rules on Auditor Independence—Frequently Asked Questions; Other Matters, Question 4 (issued December 13, 2004).

Examiners are expected to assess the adequacy of an institution's internal controls—the involved procedures, processes, and systems of its internal control structure. In so doing, they may refer to the available Internal Control Questionnaire(s) pertaining to the various transactions and activities discussed at the end of most sections of the manual. When assessing the adequacy of a bank's internal control system and structure, the examiner needs to have a good understanding of the meaning of internal control and be able to evaluate its design and effectiveness. Internal control is a process initiated by a bank's board of directors, management, and other personnel, and is designed to provide reasonable assurance that specific objectives are achieved as to the bank's (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) extent of compliance with applicable laws and regulations.[1]

The concept of control structure involves the controls that have been established and the control environment—management's monitoring of procedures, activities, and attitudes. Internal control is part of the bank's basic operations.

The components of internal control are

- *Control environment*—the environment established by the bank's employees who are responsible for its operations, including their ethical values, integrity, and competence
- *Risk assessment*—the identification, analysis, and management of risks
- *Control activities*—the institution's established policies and procedures that are designed to provide assurance that appropriate actions, which are determined by management, are taken to address identified risks
- *Information and communication*—the bank's activities that provide the basis for the gathering and exchange of information that is needed to conduct, manage, and control the organization
- *Monitoring*—the bank's continuous monitoring of the internal controls system and structure to allow for appropriate and necessary changes.

The components of internal control overlap the internal control objectives. The components of internal control must be addressed individually to assess their effectiveness relative to a specific objective.

The bank's board of directors and senior management have an important role in ensuring the adequate development, execution, maintenance, and compliance monitoring of the bank's internal controls. When determining the adequacy of a bank's management, examiners should carefully analyze and review its internal control systems, processes, and procedures.

STATEMENT ON REQUIRED ABSENCES FROM SENSITIVE POSITIONS

One of the many basic tenets of internal control is that a bank needs to ensure that its employees in sensitive positions are absent from their duties for a minimum of two consecutive weeks. Such a requirement enhances the viability of a sound internal control environment because most frauds or embezzlements require the continuous presence of the wrongdoer. After making this assessment, the bank should require that employees in sensitive key positions, such as trading and wire transfer, not be allowed to transact or otherwise carry out, either physically or through electronic access, their assigned duties for a minimum of two consecutive weeks per year. The prescribed period of absence should be sufficient to allow all pending transactions to clear. The bank should also require that an individual's daily work be processed by another employee during the employee's absence. See SR-96-37, which emphasizes the need for a bank to conduct an assessment of significant risk areas before developing a policy on required absences from sensitive positions.

A comprehensive system of internal controls is essential for a bank to safeguard its assets and capital, and to avoid undue legal risk. Senior management is responsible for establishing an appropriate system of internal controls and monitoring compliance with that system. Although no single control element should be relied on to

1. For additional information on internal controls, see the Committee of Sponsoring Organizations of the Treadway Commission's study on internal controls, *Internal Control—Integrated Framework* (AICPA, 1992).

prevent fraud and abuse, these acts are more easily perpetrated when proper segregation and rotation of duties do not exist. As a result, the Federal Reserve reemphasizes the following prudent banking practices that should be incorporated into a bank's internal control procedures. These practices are designed to enhance the viability of a sound internal control environment, as most internal frauds or embezzlements necessitate the constant presence of the offender to prevent the detection of illegal activities.

When developing comprehensive internal control procedures, each bank should first make a critical assessment of its significant areas and sensitive positions. This assessment should consider all employees, but should focus more on those with authority to execute transactions, those with signing authority and access to the books and records of the bank, as well as those employees who can influence or cause such activities to occur. Particular attention should be paid to areas engaged in trading and wire-transfer operations, including personnel who may have reconciliation or other back-office responsibilities.

After producing a profile of high-risk areas and activities, it would be expected that a minimum absence of two consecutive weeks per year be required of employees in sensitive positions. The prescribed period of absence should, under all circumstances, be sufficient to allow all pending transactions to clear and to provide for an independent monitoring of the transactions that the absent employee was responsible for initiating or processing. This practice could be implemented through a requirement that affected employees take vacation or leave, the rotation of assignments in lieu of required vacation, or a combination of both so the prescribed level of absence is attained. Some banks, particularly small community banks, might consider compensating controls such as continuous rotation of assignments in lieu of required absences to avoid placing an undue burden on the bank or its employees.

For the policy to be effective, individuals having electronic access to systems and records from remote locations must be denied this access during their absence. Similarly, indirect access can be controlled by not allowing others to take and carry out instructions from the absent employee. Of primary importance is the requirement that an individual's daily work be processed by another employee during his or her absence; this process is essential to bring to the forefront any unusual activity of the absent employee.

Exceptions to the required-absence policy may be necessary from time to time. However, management should exercise the appropriate discretion and properly document any waivers that are granted. Internal auditing should be made aware of individuals who receive waivers and the circumstances necessitating the exceptions.

If a bank's internal control procedures do not include the above practices, they should be promptly amended. After the procedures have been enhanced, they should be disseminated to all employees, and the documentation regarding their receipt and acknowledgment maintained. Additionally, adherence to the procedures should be included in the appropriate audit schedules, and the auditors should be cognizant of potential electronic access or other circumventing opportunities.

The development and implementation of procedures on required absences from sensitive positions is just one element of an adequate control environment. Each bank should take all measures to establish appropriate policies, limits, and verification procedures for an effective overall risk-management system.

1. To determine whether a critical assessment has been performed of a bank's significant areas and sensitive positions.
2. To ascertain that sound internal controls exist, including policies and procedures that provide assurances that employees in sensitive positions are absent from their duties for a minimum of two consecutive weeks per year.
3. To ascertain whether the bank has taken all measures to establish appropriate policies, limits, and verification procedures for an effective overall risk-management system.
4. To establish that the appropriate audit schedules and the audits include a review of minimum absence policies and procedures, including potential electronic access or other circumventing actions by employees.

1. Determine that a profile of high-risk areas and activities is performed on a regular, periodic basis.
2. Ascertain if employees assigned to sensitive positions are required to be absent for a minimum of two weeks per year while—
   a. pending, sensitive transactions are monitored while they clear, and
   b. daily work is monitored and processed by another employee during the regularly assigned employee's absence.
3. Determine if required internal control procedures for minimum absences (for example, rotation of assignments, vacation or leave, or a combination of both) are being used in sensitive operations such as trading, trust, wire transfer, reconciliation, or other sensitive back-office responsibilities.
4. Ascertain if appropriate policies, limits, and verification procedures have been established and maintained for an effective overall risk-management system.
5. Determine whether the bank—
   a. prohibits others from taking and carrying out instructions from the absent employees, and
   b. prevents remote electronic access to systems and records involving sensitive transactions during the regularly assigned employee's required minimum two-week absence.
6. Ascertain if waivers from the bank's two-week minimum absence policies and procedures involving sensitive positions are documented.
7. Determine that the appropriate audit schedules and the audits include a review of such procedures, including potential electronic access or other circumventing actions by employees.

The guidance[1] discussed below highlights generally the accounting and reporting requirements unique to business combinations resulting in bargain purchase gains. The guidance does not provide a comprehensive discussion on all aspects of accounting for business combinations. (See SR-10-12 and its attachment.)

SUPERVISORY CONSIDERATIONS

Compliance with GAAP and Regulatory Reporting Requirements

Accurate regulatory reports are critical for effective supervision and, because of their public availability, for enhancing the transparency of an institution's risk profile and financial position. Business combinations, including bargain purchase transactions and assisted transactions, should be accounted for in accordance with the Financial Accounting Standards Board's Accounting Standards Codification (ASC) Topic 805, "Business Combinations." The management of an acquiring institution is responsible for preparing regulatory reports in accordance with generally accepted accounting principles (GAAP), regulatory reporting requirements, and relevant supervisory guidance. The complexity of the accounting requirements related to a business combination does not relieve management of this responsibility and should be factored into management's overall analysis of the practicability of a potential acquisition. The management of each institution is responsible for establishing and maintaining appropriate governance and an effective internal control structure over the preparation of regulatory reports commensurate with the institution's size, complexity, and risk profile. This structure should include written policies and procedures that provide clear guidelines on accounting and reporting matters related to business combinations. Management is encouraged to discuss applicable regulatory reporting requirements and supervisory considerations with its primary federal regulator prior to consummating a business combination.

Fair-Value Measurements

The valuation of the assets acquired and liabilities assumed in a business combination presents accounting and supervisory challenges. For example, many of these assets and liabilities are illiquid and lack quoted market prices, which complicates the estimation of their acquisition-date fair values. Thus, a key issue underlying fair-value estimates is the appropriateness of inputs and the appropriate selection and use of valuation techniques. Some valuation techniques employ complex models and, therefore, warrant further supervisory review. For example, reliability concerns may arise when the institution does not use clear and rigorous valuation techniques or where one or more significant inputs to a valuation estimate are not observable, even indirectly, from active markets. This is especially true when estimating the fair value of illiquid financial instruments, indemnification assets, and identifiable intangible assets that are acquired in a business combination.

It is management's responsibility to report fair values in accordance with ASC Topic 820, "Fair Value Measurement." Because of the significant impact fair-value measurements and any resultant goodwill or bargain purchase gain have on the financial statements, management should have appropriate written fair-value measurement policies, procedures, and controls in place. These policies, procedures, and controls should be executed by experienced and qualified individuals knowledgeable in both GAAP and regulatory reporting requirements for business combinations. Furthermore, management's fair-value measurements should be well supported and are subject to review by examiners.

If management does not possess the expertise to identify and measure the identifiable assets acquired and the liabilities assumed in a business combination (and the equity or member interests in the acquiree in a combination of mutual institutions), management should engage a qualified third-party expert to provide professional guidance and support for the preparation

1. Part III of the June 7, 2010, "Interagency Supervisory Guidance on Bargain Purchases and FDIC- and NCUA-Assisted Acquisitions" was issued by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the former Office of Thrift Supervision.

of fair-value measurements required by ASC Topic 805 and determined in accordance with ASC Topic 820. For example, management may use a third party to estimate the expected cash flows and the fair value of a loan portfolio acquired in an assisted acquisition (and the related expected cash flows and fair value of an FDIC loss-sharing indemnification asset). The use of outside resources, however, does not relieve management of its responsibility to ensure that fair-value estimates are measured in accordance with GAAP. Management must sufficiently understand the bases for the measurement and valuation techniques used by outside parties to determine the appropriateness of these techniques, the underlying inputs and assumptions, and the resulting fair-value measurements.

Retrospective Adjustments of Fair-Value Measurements during the Measurement Period

During the measurement period, management should finalize its fair-value measurement estimates and retrospectively adjust the provisionally recorded amounts to reflect the information it was seeking about the acquisition-date facts and circumstances promptly after receipt of this information. The existence of a measurement period does not permit management to delay completion of comprehensive fair-value measurements that conform to the requirements of ASC Topic 820. Rather, at the earliest possible reporting date, management should establish and report appropriate fair-value estimates for the identifiable assets acquired and liabilities assumed in a business combination (and the equity or member interests in the acquiree in a combination of mutual institutions).

An acquiring institution's regulatory capital is subject to retrospective adjustments made during the measurement period. Although bargain purchase gains are reported in earnings and included in the computation of regulatory capital under the agencies' capital standards, the acquiring institution's primary federal regulator may determine an estimated bargain purchase gain lacks sufficient necessary permanence to rely on the estimate as a component of regulatory capital.

The Federal Reserve System relies on the timely and accurate filing of regulatory reports by domestic and foreign financial institutions. Data collected from regulatory reports facilitate early identification of problems that can threaten the safety and soundness of reporting institutions; ensure timely implementation of the prompt-corrective-action provisions required by law; and serve other legitimate supervisory purposes. Certain regulatory report information is used for public disclosure so investors, depositors, and creditors can better assess the financial condition of the reporting banks. Information that comes primarily from the Consolidated Reports of Condition and Income (Call Reports) is used to prepare the Uniform Bank Performance Report (UBPR), which employs ratio analyses to detect unusual or significant changes in a bank's financial condition as of the reporting dates. The UBPR is also used to detect changing patterns of behavior in the entire banking system; consequently, any inaccurate data in the regulatory reports may result in ratios that conceal deteriorating trends in the bank or the industry.

Generally, all regulatory reports of financial condition and income that domestic and foreign banking organizations file with the Federal Reserve are required by statute or regulation. The Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) and the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) amended various banking statutes to enhance the Federal Reserve's authority to assess civil money penalties against state member banks, bank holding companies, and foreign institutions that file "late," "false," or "misleading" regulatory reports. The civil money penalties also can be assessed against individuals who cause or participate in such filings.

The Federal Reserve has identified a late regulatory report as an official copy of a report that is not received by the Reserve Bank or its designated electronic collection agent in a timely manner. Each bank must file its Call Report in one of the following two ways:

- A bank may use computer software to prepare its report and then submit the report directly to the Federal Financial Institutions Examination Council's (FFIEC) Central Data Repository (CDR), an Internet-based system for data collection or
- The institution may complete its reports in paper form and arrange with a software vendor or another party to convert its paper reports into the electronic format that can be processed by the CDR. The software vendor or other party then must electronically submit the data file containing the bank's Call Report to the CDR.

The filing of a Call Report in paper form directly with the FDIC or with the appropriate Federal Reserve Bank is not an acceptable method of submission.

Reserve Banks will monitor the filing of all regulatory reports to ensure that they are filed, as required, on a timely basis and that they are accurate and not misleading. The Federal Reserve System's Committee on Current Series Reporting, which consists of staff from the statistics functions at each of the Reserve Banks and at the Board, will play an active role in this process. (See SR-04-15.) Many reporting errors can be screened through validity edit checks. Also, Reserve Banks have additional monitoring procedures that they use to confirm the timely submission of reports and to confirm that the reports are accurate and not misleading. On a case-by-case basis, the Reserve Banks will continue to determine if and when a financial institution or other banking organization is a chronic late, inaccurate, or false reporter; in these cases, the Banks will determine what supervisory action, if any, to recommend for a noncompliant reporter.

The filing of a false report generally involves the submission of mathematically incorrect data, such as addition errors or transpositions, or the submission of a regulatory report without its appropriate schedules. Conversely, the filing of a misleading report involves some degree of negligent behavior on the part of the filer that results in the submission of inaccurate information to the Federal Reserve.

REVIEW AND REFILING OF REGULATORY REPORTS

Review of regulatory reports involves determining whether the management of the member bank has submitted all required reports to the Federal Reserve in a timely and accurate man-

ner. The examiner assigned to a specific area of examination is responsible for reviewing the reports relating to that area and for verifying that they are accurate and meet statutory and regulatory requirements. If the examiner finds a material difference in the reports, management should be instructed to refile corrected copies, if appropriate.

Examiners should discuss on the "Examination Conclusions and Comments" and "Matters Requiring Board Attention" pages of the examination report material errors or the filing of chronically late reports. (See section 6000.1.) They should also discuss with Reserve Bank staff any regulatory report filing that is considered misleading, such a report could lead to the issuance of criminal referrals against the involved individuals. In addition, management should be reminded that civil money penalties or other enforcement proceedings could occur as a result of chronically late or false regulatory report filing.

Banks should maintain effective manual or automated internal systems and procedures to ensure that reporting meets the appropriate regulatory requirements. Banks should develop clear, concise, and orderly workpapers to support the compilation of data. Preparation of proper workpapers provides not only a logical tie between report data and the bank's financial records but also facilitates accurate reporting and verification. Ideally, as part of an effective internal control program, bank management should implement a procedure to verify the compilation of the data. At a minimum, an independent person or department should verify the data that have been compiled for inclusion in the report.

A bank's internal control and audit programs for regulatory reports should be sufficient to ensure that all required reports are submitted on time and are accurate. The specific internal controls a bank employs to meet those objectives depend largely on the volume of reports, the scope of a bank's operations, and the complexity of its accounting system.

COMMONLY REQUIRED REGULATORY REPORTS

This section describes the regulatory reports most commonly required either to be submitted by the member bank to the Federal Reserve Bank or the Board, or to be maintained by the member bank for review during an examination.

Consolidated Reports of Condition and Income

Under 12 USC 324 and the Board's Regulation H, all state member banks are required to file Consolidated Reports of Condition and Income (Call Reports) as of the last day of each calendar quarter. The specific reporting requirements, including the reporting form to be used (for example, FFIEC 031 or FFIEC 041), depend on the asset size of the bank and whether it has a foreign office. Details of the appropriate reporting guidelines, along with the specific reporting form to be filed, are found in the instructions for preparation of Reports of Condition and Income. The reporting forms and instructions can be found on the FFIEC's website: www.ffiec.gov.

The bank should submit completed Call Reports to the CDR no later than 30 calendar days after the report date. Any bank with more than one foreign office, other than a shell branch or international banking facility, must submit data to the CDR no later than 35 days after the report date. State member banks are *not* required to publish their Reports of Condition or Income, according to federal statute. However, a state member bank may be required to publish its Report of Condition under state law.

The Report of Condition provides consolidated, detailed financial information on assets, liabilities, capital, and off-balance-sheet activity, which permits a uniform analysis and comparison of the reporting bank's data to that of other insured banks. The report also aggregates certain figures on loans to executive officers, directors, principal shareholders, and their related interests. The Report of Income provides information such as consolidated earnings, changes in capital accounts and the allowance for loan and lease losses, and charge-offs and recoveries.

The examiner should carefully review both reports to ensure that all pertinent data have been reported and are properly categorized in accordance with the instructions. To understand a particular bank's Call Report, the examiner must understand the bank's accounting methods as well as the information located in, and the relationships between, the bank's general books and subsidiary ledgers. This understanding can be obtained only by a careful review of the

workpapers used in the preparation of these reports and their supplementary schedules.

REPORTS REQUIRED BY THE MONETARY CONTROL ACT OF 1980 AND THE INTERNATIONAL BANKING ACT OF 1978

The Federal Reserve has established a basic deposits-reporting framework for administering Regulation D, Reserve Requirements of Depository Institutions, and for constructing, analyzing, and controlling the monetary and reserves aggregates. The framework consists of four categories of deposit reporting. Every institution is placed into one of these four categories for deposit reporting purposes.[1] In general, the larger the institution, the more detailed or more frequent the institution will have to report.

The first two reporting categories, characterized as ''detailed reporting,'' apply to those institutions that are not exempt from reserve requirements (''non-exempt'' institutions). The last two reporting categories, characterized as ''reduced reporting,'' apply to institutions that are exempt from reserve requirements (''exempt'' institutions). The reserve-requirement ''exemption amount'' is the amount of total reservable liabilities at each depository institution that is subject to a zero-percent reserve requirement. The exemption amount is used to make the distinction between detailed deposit reporting and reduced reporting.

- Institutions with net transaction accounts equal to or less than the exemption amount over prescribed periods are exempt from reserve requirements and are subject to reduced reporting (categories 3 and 4).
- Institutions with net transaction accounts greater than the exemption amount over prescribed periods are *not* exempt from reserve requirements and are subject to detailed reporting (categories 1 and 2).

Both measures are indexed annually; see Regulation D for the appropriate exemption and cutoff amounts.

The exemption amount and the deposit cutoff for any one calendar year are used by the Federal Reserve to determine deposit-reporting panels in July, effective for September of that year, which continues to September of the following year. All deposit reports are mandatory.

Reporting Categories

''Non-exempt'' institutions subject to detailed reporting file the Report of Transaction Accounts, Other Deposits and Vault Cash (FR 2900). Institutions file the report either weekly or quarterly, generally depending on the level of an institution's deposits. The report is used in the calculation of reserve requirements.

''Exempt'' institutions subject to ''reduced reporting'' file either the Annual Report of Deposits and Reservable Liabilities (FR 2910a) or no report at all, depending on their deposit levels.

Report forms and instructions can be found on the Federal Reserve Board's website.

Category One

Depository institutions (other than banking Edge and agreement corporations and U.S. branches and agencies of foreign banks) with net transaction accounts greater than the exemption amount and with a sum of total transaction accounts, savings deposits, and small time deposits greater than or equal to the nonexempt deposit cutoff, or with a sum of total transaction accounts, savings deposits, and small time deposits greater than or equal to the reduced reporting limit, regardless of the amount of net transaction accounts, will be required to submit the FR 2900 weekly.

Banking Edge and agreement corporations and U.S. branches and agencies of foreign banks, regardless of size, must also submit the FR 2900 weekly. They are not eligible for reporting categories 2 through 4 below.

The weekly reporting period for the FR 2900 covers the seven-day period beginning on Tuesday and ending the following Monday.

Category Two

Depository institutions with net transaction accounts greater than the exemption amount and with a sum of total transaction accounts, savings deposits, and small time deposits less than the

1. Depository institutions that are required to maintain reserves are defined in section 204.1(c) of Regulation D (12 CFR 204.1(c)).

nonexempt deposit cutoff are required to submit the FR 2900 once each quarter, in March, June, September, and December.

The quarterly reporting period for the FR 2900 covers the seven-day period beginning on the third Tuesday of the report month and ending the following Monday.

Category Three

Depository institutions with net transaction accounts less than or equal to the exemption amount and with total deposits greater than the exemption amount but with total transaction accounts, savings deposits, and small time deposits below the reduced reporting limit are required to submit the FR 2910a. This report is filed as of June 30 each year.

Category Four

Depository institutions whose net transaction accounts and total deposits are less than or equal to the exemption amount are not required to submit any Federal Reserve deposit report as long as data on the level of an institution's deposits are readily available on a condition report.

Institutions for which deposit data are not readily available on a condition report will be required to submit the FR 2910a report to determine the appropriate reporting category.

See page IV-4 and IV-5 of the Federal Reserve's *Reserve Maintenance Manual* at https://www.federalreserve.gov/monetarypolicy/reserve-maintenance-manual-about-this-manual.htm.

Annual Panel Determinations

Each year the Federal Reserve reviews the institutions in the four reporting categories, and reassignments of institutions ("panel shifts") are determined each July and become effective in September. The panel shifts reflect movements in each individual depository institution's total deposits or total reservable liabilities across the prevailing boundaries (the exemption amount and the deposit cutoff) that separate the reporting categories. Documentation is available on the Federal Reserve's procedures (including the reports, data items, and reporting periods) for measuring an institution's total reservable liabilities and total deposits against the prevailing cutoffs for the annual panel determinations. Two special types of panel shifts are described below.

- *Voluntary shifts.* In July, the Federal Reserve informs each institution of its particular reporting requirement effective for September of that year to September of the following year. Any depository institution assigned to one particular category may elect instead to report deposits (and, if appropriate, to maintain reserves) in accordance with a higher-level category. (For example, an institution assigned to the FR 2900 quarterly reporting category may elect instead to report the FR 2900 weekly.) However, any such voluntary shifts may take place only once a year during the normal September panel shifts. Voluntary shifts to a lower-level category are not permitted.

- *Fast-growing institutions.* The Federal Reserve may require a depository institution that is experiencing above-normal growth to report on a more detailed or frequent basis before the September panel shifts.

For more detailed information, see the Federal Reserve's "Reserve Maintenance Manual."

REPORTS REQUIRED UNDER REGULATION H AND THE SECURITIES EXCHANGE ACT OF 1934

Section 12(i) of the Securities Exchange Act of 1934 (the 1934 act), as amended by the Sarbanes-Oxley Act of 2002, vests the Board with the authority to administer and enforce certain provisions of the 1934 act and the Sarbanes-Oxley Act with respect to state member banks that have a class of securities registered under section 12(b) or 12(g) of the 1934 act (registered state member banks). In particular, the Board is charged with enforcing sections 12, 13, 14(a), 14(c), 14(d), 14(f), and 16 of the 1934 act and sections 301, 302, 303, 304, 306(a), 401(b), 404, 406, and 407 of the Sarbanes-Oxley Act[2] with

2. See 15 USC 78j-1, 78*l*–78n, 78p, 7241–7244(a), 7261(b), 7262, 7264, and 7265.

respect to registered state member banks. Section 208.36(a) of Regulation H, which implements these provisions, generally requires registered state member banks to comply with any rules, regulations, and reporting forms adopted by the Securities and Exchange Commission (SEC) under the above-listed sections of the 1934 act and the Sarbanes-Oxley Act. (See 12 CFR 208.36(a), as amended by 68 *Fed. Reg.* 4096 (January 28, 2003).) Registered state member banks, however, generally must file any forms or reports required by these rules with the Board, rather than the SEC.

If a state member bank has a class of securities registered under section 12 of the 1934 act and, thus, is a registered state member bank, the examiner should consult with the bank's management to ensure that the reports required by Regulation H are properly filed with the Board. Listed below are a few of the most common forms and reports that must be filed with the Board by a registered state member bank pursuant to Regulation H. This list, however, is not exclusive and examiners should consult Board staff or Regulation H, the 1934 act, the Sarbanes-Oxley Act, and the SEC's implementing rules if questions arise concerning the filing of reports by a registered state member bank. See the list of reporting forms and the individual reporting forms and instructions on the SEC's website: www.sec.gov.

Section 12 of the 1934 Act

Form 8-A is for the registration of certain classes of securities pursuant to sections 12(b) or 12(g) of the 1934 act for, among other things, listing on national securities exchanges. Form F-10 is the general reporting form for registration of securities pursuant to the 1933 act and sections 12(b) or 12(g) of the 1934 act for classes of securities of issuers for which no other reporting form is prescribed.

Section 13 of the 1934 Act

Form 8-K must be filed within 4 business days after the occurrence of the earliest of one or more specified events that are required to be reported and that affect the bank or its operations, such as changes in control of registrant or an acquisition or disposition of a significant amount of assets. See the "Information to be Included in the Report" within the report instructions. Form 10-Q is for quarterly and transition reports and must be filed within 40 days for large accelerated filers; accelerated filers; or for others, 45 days after the end of each of the first three fiscal quarters. Form 10-K is for annual and transition reports that must be filed within 60 to 90 calendar days after the end of the registrant's fiscal year.

Section 16 of the 1934 Act

Section 16 requires the directors, officers, and principal shareholders of public companies to file reports concerning the purchase and sale of the company's equity securities. Form 3 collects the insider's initial beneficial ownership of registered companies, including banks. Form 4 collects changes in the insider's beneficial ownership. Form 5 is an annual statement of changes in beneficial ownership of securities.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act[3] (the act) and the SEC's implementing rules require the principal executive officer and principal financial officer of public companies to file certain certifications with the company's annual 10-K report and quarterly 10-Q reports. The certifications must, among other things, state that the officer has reviewed the report, indicate that the report (to the officer's knowledge) does not contain any material misstatements or omissions, and contain certain representations concerning the company's internal controls.

The act requires the annual 10-K report of public companies to include a statement of management's responsibility for maintaining adequate internal-control structures and procedures for financial reporting and to contain an assessment of the effectiveness of these controls and procedures.[4] The company's external auditor must attest to, and report on, management's assessment. These reports and attestations are similar to the internal-control reports and attestations required by section 36 of the Federal Deposit Insurance Act (12 USC 1831m) for

3. See 15 USC 7241 (section 302 of the act).
4. See 15 USC 7262 (section 404 of the act).

insured depository institutions with total assets of $500 million or more.

The act[5] and the SEC's rules also require public companies to disclose in their periodic reports whether the company has adopted a code of ethics for its senior financial officers and whether the company's audit committee includes a "financial expert." If the company has not adopted a code of ethics or does not have a financial expert on its audit committee, the company must explain the reasons why not.

REPORTING AND INQUIRY REQUIREMENTS FOR LOST AND STOLEN SECURITIES

Every national securities exchange member, registered securities association member, broker, dealer, municipal securities dealer, government securities broker or dealer, registered transfer agent, and registered clearing agency and its participants, as well as every member bank of the Federal Reserve System and every bank whose deposits are insured by the Federal Deposit Insurance Corporation (reporting institutions), must register with the SEC's designee, the Securities Information Center, Inc. (SIC). All lost, missing, stolen, or counterfeit securities must be reported to the SIC. Except in certain limited circumstances, each insured bank is responsible for contacting the SIC to determine if the securities coming into its possession, whether by pledge, transfer, or some other manner, have been previously reported as missing, lost, stolen, or counterfeit.

All functions within a bank that handle or process securities are subject to the *reporting* requirements. Only the transfer-agent function is exempt from the *inquiry* requirements. Accordingly, all bank departments likely to be affected, including the trust, investment, transfer-agent, custody, or dealer departments, and the lending operations as relating to collateral loans, should be familiar with the requirements set out in 17 CFR 240.17f-1. Securities exempt from the reporting requirements are—

- registered U.S. Treasury securities of the U.S. government and federal agencies thereof,
- securities that have not been assigned CUSIP numbers, and
- bond coupons
- global securities
- uncertified securities, and
- any securities issue for which there is neither a record nor beneficial owners that can obtain negotiable securities certificates.

Securities exempt from the inquiry requirements are—

- securities received directly from the issuer or its agent at issuance,
- securities received from another reporting institution or from a Federal Reserve Bank or Branch,
- securities received from a customer of the reporting institution in the name of the customer or nominee, and
- securities that are a part of a transaction of $10,000 or less (aggregate face value for bonds or market value for stocks).

Lost, Missing, Stolen, or Counterfeit Securities

Form X-17F-1A must be filed with the SIC within one business day after the discovery of—

- a theft or loss of any security when there is a substantial indication of criminal activity,
- a security that has been lost or missing for two business days when criminal actions are not suspected, and
- a security that is counterfeit.

The reporting form must be filed within two business days of notification of nonreceipt when delivery of securities sent by the bank—

- is made by mail or draft and payment is not received within 10 business days, and confirmation of nondelivery has been made by the receiving institution; and
- is in person and no receipt is maintained by the bank.

If securities sent by the bank, either in person or through a clearing agency, are lost in transit and the certificate numbers of the securities can be determined, the bank (delivering institution) must report the certificate numbers of the secu-

5. See 15 USC 7264–7265 (sections 406 and 407 of the act).

rities within two business days after notice of non-receipt or as soon as the certificate numbers of the securities can be ascertained.

When a shipment of retired securities certificates is in transit between any unaffiliated transfer agents, banks, brokers, dealers, or other reporting institutions, and the delivering institution fails to receive notice of receipt or non-receipt of the certificates, the delivering institution is required to act to determine the facts. When the certificates are not recovered by the delivering institution, the delivering institution must report the certificates as lost, stolen, or missing within a reasonable time period, but in any event within twenty business days from the date of shipment. The delivery of lost or missing securities to the bank must be reported within one business day after discovery and notification of certificate numbers. Securities that are considered lost or missing as a result of count or verifications must be reported no later than 10 business days after discovery or as soon as certificate numbers can be ascertained.

Copies of all reports required to be filed under 17 CFR 240.17f-1 must also be submitted to the registered transfer agent for the issue being reported and, if criminal activities are suspected, to the Federal Bureau of Investigation. Copies of filed or received Forms X-17F-1A must be maintained in an easily accessible place for three years.

TRANSFER-AGENT ACTIVITIES

If a bank acts as a transfer agent for its own stock, the stock of its holding company, or any other equity security, it may have to register with the Board as a transfer agent pursuant to the requirements of Regulation H (section 208.31). State member bank transfer agents must comply with the SEC's rules prescribing operational and reporting requirements, which the SEC adopted pursuant to section 17A(2) of the 1934 act (15 USC 78q-1). For member banks, see 17 CFR 240.17Ac2 (1-2) and 240.17Ad-1-240.17Ad-16). (See section 208.31(b) of Regulation H.) Any entity performing transfer agent functions for a security is required to register if the security is registered on a national securities exchange and if the issuer has total assets of $10 million and a class of equity security held on record by 500 or more persons. The registrations are public filings and are *not* confidential.

The interagency Transfer Agent Registration and Amendment Form, Form TA-1, is used by member banks and other entities to register before becoming, and then to act as, a transfer agent. They also use the reporting form to amend registration information as necessary. The information collected includes the company name, all business addresses, and information about the registrant's proposed activities as a transfer agent.

The Federal Reserve uses the information to act upon registration applications and to aid in performing supervisory duties. The Federal Reserve forwards copies of the completed registration forms to the Securities and Exchange Commission, which maintains registration data to aid in its statutory mandate to develop rules and standards applicable to all registered transfer agents.

Municipal Securities Dealer Activities

A state member bank, subsidiary, department, or division thereof that is a municipal securities dealer must register and file amendments with both the SEC and the Federal Reserve Board Board as a municipal securities dealer by filing the SEC's Form MSD, pursuant to Section 15 B(a) of the Securities Exchange Act of 1934 and the SEC's rule 15Ba2-1. A discussion of the bank's responsibilities as a municipal securities dealer, filing requirements, and other information, including examination procedures, are discussed in section 2030.1. A notice of withdrawal from registration as a municipal securities dealer pursuant to section 15B(c) must be filed with the SEC and the Board on the SEC's Form MSDW when the municipal securities dealer is a bank, or a separately identifiable department or division of a bank.

Government Securities Broker and Dealer Activities

If a state member bank, a foreign bank, a state branch or an agency of a foreign bank, or a commercial lending company owned or controlled by a foreign bank acts as a government securities broker or dealer, it may have to file notice with the Board as a government securities broker or dealer by filing FR G-FIN, pursuant to section 15C(a)(1)(B) of the Securities and

Exchange Act of 1934. This notice collects the institution's identifying information and the names and titles of its managers of government securities activities; the notice requires the institution to state whether any person associated with the respondent's government securities activities has been involved in disciplinary proceedings related to securities sales. When such a financial institution intends to cease engaging in broker or dealer activities, it must notify its regulator by using the Notice by Financial Institutions of Termination of Activities as a Government Securities Broker or Government Securities Dealer (FR G-FINW). A discussion of the bank's responsibilities as a government securities broker or dealer, filing requirements, and other information, including examination procedures, are discussed in SR-87-37, as amended. See also SR-94-5, 93-40, 90-1, and 88-26. The Board has also developed a Summary Report of Government Securities Broker/Dealer Activities (GSB-D report).

INTERNATIONAL ACTIVITIES

A bank must file certain reports if it is conducting or intends to conduct international activities through either foreign branches or Edge Act or agreement corporations. Listed below is a brief description of each of these reports.

FFIEC 009—Country Exposure Report

FFIEC 009 is filed quarterly by all U.S. banks and bank holding companies that meet certain ownership criteria and that, on a fully consolidated basis, have total outstanding claims of $30 million or more (or equivalent) on foreign residents of the U.S. Information is collected on the distribution by country of these foreign claims on foreigners held by U.S. banks and bank holding companies.

FFIEC 009a—Country Exposure Information Report

FFIEC 009a is a quarterly supplement to the Country Exposure Report (FFIEC 009) that provides specific information about the reporting institution's exposures in particular countries of U.S. banking institutions. Part A must be filed when exposure to a single country exceeds 1 percent of the banking institution's total assets or 20 percent of that institution's capital, whichever is less. Part B provides a list of countries where exposures were between 0.75 percent and 1 percent of the respondent's assets or between 15 percent and 20 percent of capital.

FFIEC 030/FFIEC 030S—Foreign Branch Report of Condition/Abbreviated Foreign Branch Report of Condition

These reports collect information on the structure and geographic distribution of foreign branch assets, liabilities, derivatives, and off-balance-sheet data of foreign branches of insured U.S.-chartered commercial banks. For purposes of this report, branches in Puerto Rico and other U.S. territories and possessions are considered foreign branches. Participation in the completion and submittal of the reports is mandatory.

The FFIEC 030 is filed quarterly for significant branches, with either $2 billion or commitments to purchase foreign currencies and U.S. dollar exchange of at least $5 billion. It is filed annually for other branches with total assets in excess of $250 million. The Federal Reserve uses the data to plan examinations and to analyze the foreign operations of domestic banks. Growth trends can be measured by bank, by country, and by bank within country. Aggregate data are a useful source of information on bank activities.

The FFIEC 030S collects financial data items for smaller, less-complex branches. It is filed annually, as of December 31, for foreign branches that do not meet the criteria to file the FFIEC 030 but have total assets of $50 million or more (but less than or equal to $250 million).

FR 2064—Recordkeeping Requirements

Effective September 1, 2001, the FR 2064 reporting form was replaced with a recordkeeping requirement and certain structure information was moved to the FR Y-10, Report of Changes in Organizational Structure. Internationally active U.S. banking organizations are still

expected to maintain adequate internal records to allow examiners to review compliance with the investment provisions of Regulation K, under the recordkeeping requirements of FR 2064 (no form is associated with this recordkeeping requirement). For each investment made under subpart A of Regulation K, records should be maintained on the type of investment (for example, equity (voting shares, nonvoting shares, partnerships, interests conferring ownership rights, participating loans)), binding commitments, capital contributions, and subordinated debt), the amount of the investment, the percentage ownership, activities conducted by the company and the legal authority for such activities, and whether the investment was made under general-consent, prior-notice, or specific-consent authority. For those investments made under general-consent authority, information also must be maintained that demonstrates compliance with the various limits set out in sections 211.8 and 211.10 of Regulation K.

Information maintained by the banking organization should be made available to examination staff during the course of on-site examinations and pursuant to other supervisory requests. The recordkeeping must be adequate to permit examiners to determine compliance. Examiners are expected to review a sample of these investments to determine the accuracy of the organization's records and to determine compliance with the regulation. (See SR-02-2.)

FR 2314/FR 2314S—Financial Statements of Foreign Subsidiaries of U.S. Banking Organizations

The FR 2314 is reported quarterly or annually, as of the last calendar day of the quarter, based on certain threshold criteria. The FR 2314 collects selected financial information for direct or indirect foreign subsidiaries of U.S. state member banks, Edge and agreement corporations, and bank holding companies. The FR 2314 consists of a balance sheet and income statement; information on changes in equity capital, changes in the allowance for loan and lease losses, off-balance-sheet items, and loans; and a memoranda section. The FR 2314S should be filed annually as of December 31 and collects four financial data items for smaller, less complex subsidiaries.

FR 2502q—Quarterly Report of Assets and Liabilities of Large Foreign Offices of U.S. Banks

The FR 2502q report is to be submitted by U.S. head offices of bank holding companies, commercial banks, and Edge and agreement corporations that file for their major foreign branches and large banking subsidiaries. It provides a geographic breakdown of each office's assets and liabilities. Branches of a U.S. bank with $500 million or more in total assets and foreign banking subsidiaries with $2 billion or more in total assets, or $10 million in deposit liabilities, are required to file this report quarterly.

FR 2886b—Consolidated Report of Condition and Income for Edge Act and Agreement Corporations

FR 2886b covers the operations of the reporting corporation, including any international banking facilities of the reporter. Corporations engaged in banking must submit the data at least quarterly.

FR 2915—Report of Foreign Currency Deposits

FR 2915 collects seven-day averages of the amounts outstanding of foreign currency–denominated deposits held at U.S. offices of the depository institution, converted to U.S. dollars and included in the Report of Transaction Accounts, Other Deposits and Vault Cash (FR 2900). The report is collected with the reporting week that begins the third Tuesday of March, June, September, and December.

FR Y-10—Report of Changes in Organizational Structure

The Y-10 is used to report, among other things, information on worldwide organizational structure of bank holding companies (BHCs), member banks, Edge and agreement corporations, and the U.S. operations of foreign banking organizations (FBOs)[6]. The reporting form

6. An FBO with U.S. operations that is not or ceases to be a "qualifying foreign banking organization" (QFBO) within

includes detailed information on the structure of top-tier BHCs organized under U.S. or foreign law that are not FBOs, regardless of financial holding company (FHC) status; FBOs (both qualifying and nonqualifying) whether or not a BHC; state member banks not controlled by a BHC or FBO; Edge and agreement corporations not controlled by a BHC, FBO, or member bank; and nationally chartered banks not controlled by a BHC or FBO, but only with respect to their foreign investments. Within 30 calendar days of the event, banking organizations are required to report changes in investments as well as new activities (both foreign and domestic) on the FR Y-10 report. The reporting form includes the structure information on changes in FBOs (formerly the FR Y-10F) and the change in status of foreign branch of U.S. banking organizations (formerly the FR 2058).

The Board has placed greater importance on monitoring the level of international investments to ensure compliance with relevant banking laws and regulations, and to ensure that banking organizations do not expose themselves to undue risk. Examiners and other Federal Reserve System staff have a continuing need to monitor compliance with the Federal Reserve Act and sections 211.8–211.10 of the revised Regulation K.

Investments of less than 25 percent of the voting shares of a foreign nonbanking company are reported on the FR Y-10.[7] However, using the FR Y-6 (Annual Report of Bank Holding Companies) and the FR Y-7 report (Annual Report of Foreign Banking Organizations), banking organizations are required to report annually all investments, including those between 5 percent and 25 percent of voting shares.[8] The FR Y-6, FR Y-7, and the FR Y-10 collect information on structure and geographical information relating to foreign investments for ongoing monitoring.

Examiners are expected to review investment amounts and activities during the examination process. The portion of an examination dealing with Regulation K compliance should focus on confirming investments made pursuant to the general-consent provisions to meet the restrictions on investment amount and activities in sections 211.8–211.10 of Regulation K. Investments made under the general-consent provisions of Regulation K can be sizable, and thus can pose significant risk to the banking organization. Examiners should keep in mind that the Board has the authority to rescind an organization's general-consent investment privileges for various reasons, including safety-and-soundness concerns and noncompliance with the existing requirements of Regulation K. (See SR-02-2.)

Treasury International Capital Forms

The following reports are collected to gather information on international capital movements by U.S. banks and their Edge Act and agreement corporations, other depository institutions, international banking facilities, and bank holding companies.

- BC: Report of U.S. Dollar Claims of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers, and Dealers on Foreigners
- BL-1: Report of U.S. Dollar Liabilities of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers, and Dealers to Foreign-Residents
- BL-2: Report of Customers' U.S. Dollar Liabilities to Foreigners
- BQ-1: Report of Customers' U.S. Dollar Claims on Foreigners
- BQ-2: Part 1. Report of Foreign Currency Liabilities and Claims of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers and Dealers, and of Their Domestic Customers vis-à-vis Foreigners
- BQ-2: Part 2. Report of Customers' Foreign Currency Liabilities to Foreigners
- BQ-3: Report of Maturities of Selected Liabilities of Depository Institutions, Bank Holding Companies/Financial Holding Companies, Brokers, and Dealers to Foreigners

the meaning of Regulation K, and is not otherwise treated as a QFBO under Regulation K, should consult with Federal Reserve staff regarding the scope of its reporting obligations. In general, an FBO that is not or is not treated as a QFBO is subject to the nonbanking restrictions of the BHC Act with respect to its worldwide operations and, thus, would have to report on the FR Y-10 changes to its worldwide organizational structure.

7. Regulation K authorizes portfolio investments in less than 20 percent of the shares of a foreign company regardless of the activities engaged in by that company. Portfolio investments within the general-consent limits are required to be reported annually on the FR Y-6.

8. Investments representing less than 5 percent ownership are not required to be reported.

D: Report of Holdings of, and Transactions in, Financial Derivatives Contracts

S: Purchases and Sales of Long-Term Securities by Foreign-Residents

SHC/SHCA: Report of U.S. Ownership of Foreign Securities, Including Selected Money Market Instruments

SHL/SHLA: Foreign-Residents' Holdings of U.S. Securities, Including Selected Money Market Instruments

Consolidated Foreign Currency Reports of Major Market Participants

The Treasury Foreign Currency (TFC) Report of major market participants collects data on the foreign exchange contracts and actively manages positions of major nonbank market participants. This report is collected and processed by the Federal Reserve System, acting as fiscal agent for the Department of the Treasury. These data are designed to assess and monitor the foreign exchange developments in the spot, forward, futures, and options markets on an individual and aggregate basis. The TFC series is comprised of three reports: (1) the Weekly Consolidated Foreign Currency Report of Major Market Participants (TFC-1), (2) the Monthly Consolidated Foreign Currency Report of Major Market Participants (TFC-2), and (3) the Quarterly Consolidated Foreign Currency Report (TFC-3).

Key Financial Accounting Standards Board (FASB) Accounting Standards Codification (ASC)® References

In June 2009, the FASB issued Statement No. 168, The FASB Accounting Standards Codification® and the Hierarchy of Generally Accepted Accounting Principles (FAS 168), to establish the FASB Codification as the single source of authoritative nongovernmental U.S. generally accepted accounting principles. The FASB Codification is effective for interim and annual periods ending after September 15, 2009. The following table is largely applicable to Call Reports and other regulatory reports, which are discussed in more detail in section 4150 of this manual. The table can also be used for precodification FASB references that are found throughout the *Commercial Bank Examination Manual*. More information regarding the FASB ASC Codification can be accessed at http://asc.fasb.org/.

Precodification Reference/Description			*Codification Topic*		*Codification Subtopic*	
SFAS	5	Accounting for Contingencies	310	Receivables	10	Overall
			450	Contingencies	20	Loss Contingencies
SFAS	13	Accounting for Leases	840	Leases		
SFAS	15	Accounting for Debtors and Creditors for Troubled Debt Restructurings	310	Receivables	40	Troubled Debt Restructurings by Creditors
SFAS	28	Accounting for Sales with Leasebacks	840	Leases	40	Sale-Leaseback Transactions
SFAS	34	Capitalization of Interest Costs	835	Interest	20	Capitalization of Interest
SFAS	52	Foreign Currency Translation	830	Foreign Currency Matters		

Precodification Reference/Description			*Codification Topic*		*Codification Subtopic*	
SFAS	65	Accounting for Certain Mortgage Banking Activities (as amended by SFAS 140)	948	Financial Services – Mortgage Banking		
SFAS	66	Accounting for Sales of Real Estate	360	Property, Plant, and Equipment	20	Real Estate Sales
SFAS	72	Accounting for Certain Acquisitions of Banking and Thrift Institutions	805	Business Combinations		
SFAS	86	Accounting for the Costs of Computer Software to Be Sold, Leased, or Otherwise Marketed	985	Software	20	Costs of Software to Be Sold, Leased or Marketed
SFAS	87	Employer's Accounting for Pensions	715	Compensation – Retirement Benefits		
SFAS	91	Accounting for Nonrefundable Fees and Costs Associated with Originating or Acquiring Loans and Initial Direct Costs of Leases	310	Receivables	20	Nonrefundable Fees and Other Costs
SFAS	94	Consolidation of All Majority-owned Subsidiaries	810	Consolidation	10	Overall
SFAS	106	Employer's Accounting for Postretirement Benefits Other Than Pensions	715	Compensation – Retirement Benefits		
SFAS	109	Accounting for Income Taxes	740	Income Taxes		
SFAS	114	Accounting by Creditors for Impairment of a Loan	310	Receivables		
SFAS	115	Accounting for Certain Investments in Debt and Equity Securities	320	Investments – Debt and Equity Securities		
SFAS	125	Accounting for Transfers and Servicing of Financial Assets and Extinguishments of Liabilities (superseded by SFAS 140)	860	Transfers and Servicing		
SFAS	133	Accounting for Derivative Instruments and Hedging Activities (as amended by SFAS 149)	815	Derivatives and Hedging		
SFAS	140	Accounting for Transfers and Servicing of Financial Assets and Extinguishments of Liabilities (as amended by SFAS 166)	860	Transfers and Servicing		
			405	Liabilities	20	Extinguishments of Liabilities
SFAS	141R	Business Combinations	805	Business Combinations		

Precodification Reference/Description			*Codification Topic*		*Codification Subtopic*	
SFAS	142	Goodwill and Other Intangible Assets	350	Intangibles – Goodwill and Other		
SFAS	144	Accounting for the Impairment of Long-Lived Assets	360	Property, Plant, and Equipment		
SFAS	149	Amendment of Statement 133 on Derivative Instruments and Hedging Activities	815	Derivatives and Hedging	10	Overall
SFAS	154	Accounting Changes and Error Corrections	250	Accounting Changes and Error Corrections		
SFAS	155	Accounting for Certain Hybrid Financial Instruments	815	Derivatives and Hedging	15	Embedded Derivatives
SFAS	156	Accounting for Servicing of Financial Assets	860	Transfers and Servicing	50	Servicing Assets and Liabilities
SFAS	157	Fair Value Measurements	820	Fair Value Measurements and Disclosures		
SFAS	159	Fair Value Option	825	Financial Instruments	10	Overall
SFAS	166	Accounting for Transfers of Financial Assets	860	Transfers and Servicing	10	Overall
			320	Investments – Debt and Equity Securities		
SFAS	167	Amendments of FASB Interpretation No. 46(R)	810	Consolidation	10	Overall
DIG	Issue B40	Application of Paragraph 13(b) to Securitized Interests in Prepayable Financial Assets	815	Derivatives and Hedging	15	Embedded Derivatives
EITF	90-5	Exchanges of Ownership Interests between Entities under Common Control	852	Reorganizations	10	Overall
EITF	96-19	Debtor's Accounting for a Modification or Exchange of Debt Instruments	470	Debt	50	Modification and Extinguishments
EITF	99-20	Recognition of Interest Income and Impairment on Purchased and Retained Interests in Securitized Financial Assets	325	Investments – Other	40	Beneficial Interests in Securitized Financial Assets
EITF	03-16	Accounting for Investments in Limited Liability Companies	323	Investments – Equity Method and Joint Ventures	30	Partnerships, Joint Ventures and Limited Liability Entities

Precodification Reference/Description			*Codification Topic*		*Codification Subtopic*	
EITF	06-4	Accounting for Deferred Compensation and Postretirement Benefit Aspects of Endorsement Split-Dollar Life Insurance Arrangements	715	Compensation – Retirement Benefits	60	Defined Benefit Plans – Other Postretirement
EITF	06-5	Accounting for Purchases of Life Insurance – Determining the Amount That Could Be Realized in Accordance with FASB TB 85-4	325	Investments – Other	30	Investments in Insurance Contracts
EITF	06-10	Accounting for Deferred Compensation and Postretirement Benefit Aspects of Collateral Assignment Split-Dollar Life Insurance Arrangements	715	Compensation – Retirement Benefits	60	Defined Benefit Plans – Other Postretirement
EITF	Topic D-46	Accounting for Limited Partnership Investments	323	Investments – Equity Method and Joint Ventures	30	Partnerships, Joint Ventures and Limited Liability Entities
EITF	Topic D-97	Push-Down Accounting	805	Business Combinations	50	Related Issues
TB	85-4	Accounting for Purchases of Life Insurance	325	Investments – Other	30	Investments in Insurance Contracts
INT	14	Reasonable Estimation of the Amount of a Loss	450	Contingencies	20	Loss Contingencies
INT	39	Offsetting of Amounts Related to Certain Contracts	210	Balance Sheet	20	Offsetting
INT	41	Offsetting of Amounts Related to Certain Repurchases and Reverse Repurchase Agreements	210	Balance Sheet	20	Offsetting
INT	48	Accounting for Uncertainty in Income Taxes	740	Income Taxes	10	Overall
ARB	43	Chapter 1, Section B	505	Equity	30	Treasury Stock
APBO	12	Omnibus Opinion – 1967	710	Compensation-General	10	Overall
APBO	16	Business Combinations	805	Business Combinations		
APBO	17	Intangible Assets	350	Intangibles – Goodwill and Other		
APBO	20	Accounting Changes	250	Accounting Changes and Error Corrections		
APBO	21	Interest on Receivables and Payables	835	Interest	30	Imputation of Interest
APBO	25	Accounting for Stock Issued to Employees	718	Compensation – Stock Compensation		

Precodification Reference/Description			*Codification Topic*		*Codification Subtopic*	
APBO	30	Reporting the Results of Operations	225	Income Statement	20	Extraordinary and Unusual Items
PB	4	Accounting for Foreign Debt/Equity Swaps	942	Financial Services – Depository and Lending	310	Receivables
PB	6	Amortization of Discounts on Certain Acquired Loans*				
PB	11	Accounting for Preconfirmation Contingencies in Fresh-Start Reporting	852	Reorganizations	10	Overall
SOP	90-7	Financial Reporting by Entities in Reorganization Under the Bankruptcy Code	852	Reorganizations	10	Overall
SOP	92-3	Accounting for Foreclosed Assets (superseded by SFAS 144)*				
SOP	93-6	Employers' Accounting for Employee Stock Ownership Plans	718	Compensation – Stock Compensation	40	Employee Stock Ownership Plans
SOP	98-1	Accounting for the Costs of Computer Software Developed or Obtained for Internal Use	350	Intangibles – Goodwill and Other	40	Internal-Use Software
SOP	98-5	Reporting on the Costs of Start-Up Activities	720	Other Expenses	15	Start-Up Costs
SOP	03-3	Accounting for Certain Loans or Debt Securities Acquired in a Transfer	310	Receivables	30	Loans and Debt Securities Acquired with Deteriorated Credit Quality

Notes:
APBO Accounting Principles Board Opinion
ARB Accounting Research Bulletin
DIG Derivatives Implementation Group
EITF Emerging Issues Task Force
INT FASB Interpretation
PB AICPA Practice Bulletin
SFAS Statement of Financial Accounting Standards
SOP AICPA Statement of Position
TB FASB Technical Bulletin
* Precodification Standard referenced in the Call Report instructions, but not codified in the Accounting Standards Codification

1. To determine that required reports are being filed on time.
2. To determine that the contents of reports are accurate.
3. To effect corrective action when official reporting, practices, policies, or procedures are deficient.

1. Complete or update the Internal Control Questionnaire, if selected for implementation.
2. Determine the bank's historical record of submitting timely and accurate reports by reviewing workpapers and the Regulatory Reports Monitoring Program.
3. Instruct those examiners assigned specific departments that generate regulatory reports to:
   a. Determine from department records what regulatory reports should have been filed because of the passage of time or the occurrence of an event.
   b. Obtain copies of all regulatory reports filed by the department since the previous examination.
   c. Check the reports obtained in the preceding step and the date of filing against statutory and regulatory requirements.
   d. Instruct the bank to prepare and submit any delinquent reports.
   e. For the most recent filing of those reports submitted on a periodic basis and all other reports submitted since the last examination, perform the following:
      - Reconcile the line items shown on the reports to the bank's general ledger, subsidiary ledgers, or daily statements.
      - Obtain the bank's workpapers applicable to each line item and reconcile individual items to the reports.
      - Determine whether other examining personnel uncovered any misstatement of assets, liabilities, income, or expense during their examination of the various departments.
      - Determine that the reports are prepared in accordance with Federal Reserve and/or other applicable instructions.
   f. On the basis of the work performed in the preceding step, perform either of the following, as appropriate:
      - If the reports are found to be substantially correct, limit the review of the remaining periodic reports filed since the last examination to the reconciliation of financial statement account categories to general ledger control accounts.
      - If the reports are found to be substantially incorrect, extend the procedures outlined in step 3.e to the remaining periodic reports filed since the last examination for those areas where items were found to be substantially incorrect.
   g. Scan all periodic reports for unusual fluctuations. Investigate fluctuations, if any.
4. Review compliance with the missing, lost, counterfeit, or stolen securities requirements of 17 CFR 240.17f-1 by:
   a. Discussing with appropriate officers and personnel the procedures in effect regarding the filing of Form X-17F-1A (Missing, Lost, Stolen, or Counterfeit Securities Report).
   b. Discussing with the appropriate persons the procedures in effect regarding compliance with the inquiry requirements.
   c. Substantiating Internal Control questions 6 through 15, as appropriate.
5. Prepare comments in appropriate report form and discuss with management:
   a. Violations of law or regulations.
   b. Inaccurate reports, and, if applicable, the need for amended reports. If amended reports are considered appropriate, consult with Reserve Bank supervisory personnel before requesting the bank to refile the report(s).
   c. Material differences in the annual report of the state member bank whose securities are subject to registration pursuant to the Securities Exchange Act of 1934. (State law governs the furnishing of annual reports to stockholders for banks with less than 500 shareholders.)
   d. Recommended corrective action when policies, practices, or procedures are deficient or when reports have been filed incorrectly, late, or not at all.

   The comments must include, if applicable, the name(s) and the "as of" date(s) of amended report(s); and the date of filing, amount of, and explanation of any material difference existing in either the numerical items or narrative statements in the annual report.
6. Update the workpapers with any information that will facilitate future examinations.

Review of Regulatory Reports

Internal Control Questionnaire

Effective date May 1993

Section 4550.4

Review the bank's internal controls, policies, practices, and procedures for regulatory reports. The bank's system should be documented in a complete and concise manner and should include, where appropriate, narrative descriptions, flowcharts, copies of forms used, and other pertinent information.

1. Do requests for all regulatory reports come to one individual or department?
2. Does that individual or department have the authority to request that required information be prepared by the applicable banking department?
3. To ensure that all regulatory reports are submitted on a timely basis and are accurate, determine the following:
   a. If completion of the report requires information from several departments:
      - Is a written memorandum sent to the various departments requesting the information?
      - Is the memorandum addressed to a department head?
      - Does the memorandum have a due date?
      - Are procedures in effect to send second requests if the memorandum is not returned by its original due date?
      - Does completion of the memorandum require two signatures, that of the person gathering the information and that of the person's superior who is held responsible for its accuracy?

   b. If completion of the report requires information from one department, is there separation of duties to ensure that the raw data to complete the report is compiled by one person and verified by another person, prior to submission?
4. After the report is prepared, but prior to its submission, is it checked by:
   a. The supervisor of the department preparing the report, who takes personal responsibility for its accuracy and submission on a timely basis?
   b. Bank personnel who have no part in the report's preparation?
5. Do report workpapers leave a clear audit trail from the raw data to the finished report and are they readily available for inspection?

   Review the bank's system for compliance with the reporting and inquiry requirements of the lost and stolen securities provisions of 17 CFR 240.17f-1.
6. Has the bank registered as a direct or indirect inquirer with the Securities Information Center, Inc.?
7. Are reports submitted within one business day of discovery when:
   a. Theft or loss of a security is believed to have occurred through criminal activity?
   b. A security has been missing or lost for two business days, except in certain cases?
   c. A security is counterfeit?
8. Are reports submitted by the bank, as a delivering institution, within two business days of notification of nonreceipt when:
   a. Delivery is in person and no receipt is maintained by the bank?
   b. Delivery of securities is made by mail or via draft, and payment is not received within 10 business days and confirmation of nondelivery has been made by the receiving institution?
   c. Securities are lost in transit and the certificate number(s) can be determined?
9. Are reports submitted by the bank, as a receiving institution, within one business day of discovery and notification of the certificate number(s) when:
   a. Securities are delivered through a clearing agency and the delivering institution has supplied the certificate numbers within the required two business days after request?
   b. Securities are delivered over the window and the delivering institution has a receipt and supplies the certificate number(s) within the required two business days after request?
10. Are securities that are considered to be lost or missing as a result of counts or verifications reported no later than ten business days after discovery or as soon after as the certificate number(s) can be ascertained?
11. Are copies of those reports submitted to the registered transfer agent for the issue and, in

the case of suspected criminal activity, the Federal Bureau of Investigation?

12. Are all recoveries of securities reported within one business day of recovery or finding? (Note: Only the institution that initially reported the security as missing can make a recovery report.)
13. Are inquiries made when the bank takes in any security that is not:
    a. Received directly from the issuer or issuing agent at issuance?
    b. Received from another reporting institution or Federal Reserve bank in its capacity as fiscal agent?
    c. Received from a bank customer and is registered in the name of the customer or its nominee?
14. Are all reports made on Form X-17F-1A or facsimile?
15. Are copies of Form X-17F-1A and subsequent confirmations and other information received maintained for three years in an easily accessible location?

CONCLUSION

16. Does the foregoing information provide an adequate basis for evaluating internal controls in that deficiencies in areas not covered by this questionnaire do not significantly impair any controls? Explain negative answers briefly, and indicate any additional examination procedures deemed necessary.
17. Are internal controls adequate based on a composite evaluation, as evidenced by answers to the foregoing questions?

To meet competitive pressures, banks provide a large number of customer services that normally do not result in assets and liabilities subject to entry on the general ledger, but that may involve significant risk. These customer services include fiduciary accounts, investment management, customer safekeeping, rental of safe deposit box facilities, purchase and sale of investments for customers, sale of traveler's checks, and collection department services. The bank is responsible for properly maintaining and safeguarding all consigned items. Banks accomplish the necessary control and review of consigned and collection items through non-ledger control or memorandum accounts. Automated systems, such as a Securities Movements Accounting and Control system (SMAC), can provide proper control for fiduciary, customer safekeeping, custodial, and investment management accounts.

CUSTOMER SAFEKEEPING

Custodial and Investment Management Accounts

Banks may act as custodians for customers' investments such as stocks, bonds, or gold. Custodial responsibilities may involve simple physical storage of the investments, as well as recording sales, purchases, dividends, and interest.[1] On the other hand, responsibilities may be expanded to include actually managing the account. This type of account management includes advising customers when to sell or buy certain investments, as well as meeting their recording requirements. In addition, the bank may lend securities from custodial accounts if authorized by the customer. This transaction allows the bank, as custodian, to charge a fee for lending the securities, thereby reducing its net custody costs. Also, both the bank and the custodial account benefit from interest earned on the transaction. This type of transaction should be governed by a policy that clearly specifies quality and maturity parameters. Additionally, to prevent defaults, borrowers should be subject to minimum credit standards, ongoing financial monitoring, and aggregate borrowing limits. Banks may also indemnify customer accounts against losses from a borrower or collateral default. Such indemnification creates a contingent financial risk to the institution.

Before providing such management and/or lending services, the bank should seek the advice of legal counsel about applicable state and federal laws concerning that type of bank-customer relationship. In addition, the use of signed agreements or contracts that clearly define the services to be performed by the bank is a vitally important first step in limiting the bank's potential liability and risk. The bank must also ensure that a proper control environment, including joint custody and access procedures, is established and maintained in support of custodial and management activities. Clearly, the largest and most active companies take on an increased level of risk. For companies that are aggressively pursuing custodial services or other nontraditional lines of business, the examiner should consider an expanded scope of review for these activities.

Safe Deposit Boxes

When banks maintain safe deposit box facilities, the bank and the customer enter into a contract whereby the bank receives a fee for renting safe deposit boxes. The bank assumes the responsibility of exercising reasonable care and precaution against loss of the box's contents. When a loss does occur, unless the bank can demonstrate it has maintained the required standard of care, it could be held liable for the loss. The required standard of care is defined as that which would be taken by a reasonably prudent and careful person engaged in the same business. Two different keys are required to open the box, and the customer and the bank each have one. Careful verification of a customer's identification is critical to meeting an appropriate standard of care. The customer is not required to disclose the contents of the box to the bank and upon court order the bank may gain access to the box without the presence of the customer.

1. Collection of interest and dividend income cannot be facilitated by the bank where the securities held are still in the customer's name, unless the paying agent is advised to change the dividend/interest address. Typically, when securities remain in the registered name of the holder, the holder continues to receive the dividend/interest payments. If the securities are re-registered into the name of the bank (or its nominee), then dividends and interest are received by the bank for the credit of the custodial customer.

Safekeeping

In addition to items held as collateral for loans, banks occasionally hold customers' valuables for short periods of time. The bank may or may not charge a fee for the service. Although it is a convenience for bank customers, many banks attempt to discourage the practice by emphasizing the benefits of a safe deposit box. When it is not possible or practical to discourage a customer, the same procedures that are employed in handling collateral must be followed. Items to be stored should be inventoried by two persons and maintained under dual control in the bank's vault. A multicopy, prenumbered, safekeeping receipt should be prepared with a detailed description of the items accepted and it should be signed by the customer. Sealed packages with contents unknown to the bank should never be accepted for safekeeping.

COLLECTION ITEMS

The collection department is one of the most diversified areas in the bank. It engages in receiving, collecting, and liquidating items which generally require special handling and for which credit normally is given only after final payment is received. The bank acts as agent for its customers or correspondents and receives a fee for that service. Even though general ledger accounts rarely are used in the collection process, the importance and value of customer assets under bank control demand the use of accounting procedures adequate to provide a step-by-step historical summary of each item processed. An audit trail must be developed to substantiate the proper handling of all items and to reduce the bank's potential liability.

CONSIGNED ITEMS

The most common items held on consignment by banks are unissued gift or traveler's checks; commemorative coins, postage stamps, and other consigned or promotional assets; and gold. Traveler's checks may be useful to customers because of the possibility that customers can obtain a refund if the checks are lost or stolen. Traveler's checks are issued for a fee or commission shared by the consignor and the issuing bank. Generally, a working supply of the checks is maintained at the teller line or selling station and a reserve supply is maintained under dual control in the bank's vault.

Under paragraph 7 of section 5136 of the Revised Statutes, national banks may exercise their powers ''by buying and selling exchange, coin and bullion.'' This statute is applied to state member banks under section 9, paragraph 20, of the Federal Reserve Act. Consequently, banks may deal only in gold or silver that qualifies as coin or bullion. The term ''coin'' means coins minted by a government or exact restrikes, minted at a later date by, or under the authority of, the issuing government.

Rarely does a bank receive sufficient revenues from the above transactions to cover the cost of handling them. However, banks must offer a full range of services to be competitive and attract customers. The bank assumes the responsibility and related contingent liability to properly maintain the assets of others and to properly record all transactions involved with the consigned items.

INTERNAL CONTROL CONSIDERATIONS

It is essential that bank policy provides for proper internal controls, operating procedures, and safeguards. In all cases, control totals must be generated and the function balanced periodically by someone not associated with the function. Proper insurance protection must also be obtained to protect against claims arising from mishandling, negligence, mysterious disappearance, or other unforeseen occurrences. If an employee should, by fraud or negligence, permit unauthorized removal of items held for safekeeping or issue traveler's checks improperly, the bank may be held liable for losses. Therefore, banks should maintain adequate bonding for contingent liabilities and the examiner should review applicable insurance policies.

Other Non-Ledger Control Accounts
Examination Objectives
Effective date May 1996

Section 4560.2

1. To determine if the policies, practices, procedures, and internal controls regarding custodial activities, consigned items, and other non-ledger control accounts are adequate.
2. To determine if bank officers and employees are operating in conformance with the established guidelines.
3. To determine the scope and adequacy of the audit function.
4. To determine compliance with laws and regulations.
5. To initiate corrective action when policies, practices, procedures, or internal controls are deficient or when violations of laws or regulations have been noted.

1. If selected for implementation, complete or update the Consigned Items and Other Non-Ledger Control Accounts section of the Internal Control Questionnaire.
2. Based on the evaluation of internal controls and the work performed by internal/external auditors, determine the scope of the examination.
3. Test for compliance with policies, practices, procedures and internal controls in conjunction with performing the remaining examination procedures. Obtain a listing of any deficiencies noted in the latest review done by internal/external auditors from the examiner assigned ''Internal Control'' and determine if appropriate corrections have been made.
4. Obtain a listing of consigned items or assets, payment instruments, and other non-ledger control accounts from the bank.
5. Scan any existing control accounts for any significant fluctuations and determine the cause of fluctuations.
6. Compare bank control records to remittance records for unissued U.S. savings bonds and state-issued food stamp value-payment cards or instruments.
7. Determine compliance with laws and regulations pertaining to non-ledger control accounts by determining, through observation and discussion with management, that there exist no violation of the prohibition against a bank participating in lotteries (section 9A of the Federal Reserve Act (12 USC 25A)).
8. Prepare in appropriate report form, and discuss with appropriate officer(s):
   a. Violations of laws and regulations.
   b. Recommended corrective action when policies, practices or procedures are deficient.
9. Update the workpapers with any information that will facilitate future examinations.

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

SAFE DEPOSIT BOXES

1. Has counsel reviewed and approved the lease contract in use which covers the rental, use and termination of safe deposit boxes?
*2. Is a signed lease contract on file for each safe deposit box in use?
3. Are receipts for keys to the safe deposit box obtained?
4. Are officers or employees of the bank prohibited from acting as a deputy or having the right of access to safe deposit boxes except their own or one rented in the name of a member of their family?
5. Is the guard key to safe deposit boxes maintained under absolute bank control?
6. Does the bank refuse to hold, for renters, any safe deposit box keys?
7. Is each admittance slip signed in the presence of the safe deposit clerk and the time and date of entry noted?
8. Are admittance slips filed numerically?
9. Are vault records noted for joint tenancies and co-rental contracts requiring the presence of two or more persons at each access?
10. Are the safe deposit boxes locked closed when permitting access and the renter's key removed and returned to the customer?
11. Is the safe deposit clerk prohibited from assisting the customer in looking through the contents of a box?
12. Does the safe deposit clerk witness the relocking of the box?
13. Are all coupon booths examined by an attendant after being used but before being assigned to another renter, to be sure the previous person did not leave behind anything of value?
14. Has a standard fee schedule for this service been adopted?
15. Are all collections of rental income recorded when received?
16. Are all safe deposit boxes where lessee is delinquent in rent, flagged or otherwise marked so that access will be withheld until rent is paid?
17. Is there a file maintained of all attachments, notices of bankruptcy, letters of guardianship and letters testamentary served on the bank?
18. Is an acknowledgment of receipt of all property, and a release of liability signed upon termination of occupancy?
19. Are locks changed when boxes are surrendered, whether or not keys are lost?
20. Is drilling of boxes witnessed by two individuals?
21. Are the contents of drilled boxes inventoried, packaged, and placed under dual control?
*22. Are all extra locks and keys maintained under dual control?

Conclusion

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

ITEMS IN SAFEKEEPING

*25. Are such items segregated from bank-owned assets and maintained under dual control?
26. Is there a set charge or schedule of charges for this service?

27. Do bank policies prohibit holding items in safekeeping free of charge?
28. Are duplicate receipts issued to customers for items deposited in safekeeping?
29. Are the receipts prenumbered?
*30. Is a safekeeping register maintained to show details of all items for each customer?
*31. Is a record maintained of all entries to custodial boxes or vaults?
32. Does the bank refuse to accept sealed packages when the contents are unknown?
33. If the bank has accepted sealed packages for safekeeping, the contents of which are not described, has the approval of the bank's counsel been obtained?
34. When safekeeping items are released, are receipts obtained from the customer?

Conclusion

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

CUSTODIAN ACCOUNTS

(Omit this section if the bank's trust department handles such accounts).

*37. Does the bank have written contracts on hand for each account that clearly define the functions to be performed by the bank?
38. Has bank counsel reviewed and approved the type and content of the contracts being used?
39. Does the bank give customers duplicate receipts with detailed descriptions, including dates of coupons attached, if applicable, for all items accepted?
40. Are those receipts prenumbered?
41. Do bank procedures prohibit its holding any investments not covered by a sale or purchase order in this department?
42. Are all orders for the purchase and sale of investments properly authorized in the account contract or signed by customers?
43. For coupon securities held by the bank:
    a. Is a tickler file or other similar system used to ensure prompt coupon redemption on accounts where the bank has been authorized to perform that service?
    b. Are procedures in effect to prevent clipping of coupons where bank is not so authorized?
    c. Have procedures been adopted to insure prompt customer credit when coupon proceeds or other payments are received?
*44. Are all investment items handled in this area maintained under dual control?
45. Have procedures been established for withdrawal and transmittal of items to customers?
*46. Does an officer review and approve all withdrawals prior to the transaction?
47. Has a standard fee schedule for this service been adopted?

Conclusion

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

COLLECTION ITEMS

50. Is access to the collection area controlled (if so, indicate how)?
*51. Are permanent registers kept for incoming and outgoing collection items?
52. Are all collections indexed in the collection register?
53. Do such registers furnish a complete history of the origin and final disposition of each collection item?

54. Are receipts issued to customers for all items received for collection?
55. Are serial numbers or prenumbered forms assigned to each collection item and all related papers?
*56. Are all incoming tracers and inquiries handled by an officer or employee not connected with the processing of collection items?
57. Is a record kept to show the various collection items which have been paid and credited as a part of the day's business?
58. Is an itemized daily summary made of all collection fees, showing collection numbers and amounts?
59. Are employees handling collection items periodically rotated, without advance notification, to other banking duties?
*60. Is the employee handling collection items required to make settlement with the customer on the same business day that payment of the item is received?
61. Does the bank have an established policy of not allowing the customer credit until final payment is received?
*62. Have procedures been established, including supervision by an officer, for sending tracers and inquiries on unpaid collection items in the hands of correspondents?
63. In the event of nonpayment of a collection item, is the customer notified and the item promptly returned?
*64. Are the files of notes entered for collection clearly and distinctly segregated from bank-owned loans and discounts?
*65. Are collection notes above maintained under memorandum control and is the control balanced regularly?
66. Are collection files locked when the employee handling such items is absent?
67. Are vault storage facilities provided for collection items carried over to the next day's business?
*68. Does the collection teller turn over all cash to the paying teller at the close of business each day and start each day with a standard change fund?
69. Has a standard fee schedule for this service been adopted?
70. Is the fee schedule always followed?
71. Is a permanent record maintained for registered mailed?

Conclusion

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

CONSIGNED ITEMS

*74. Is the reserve stock of consigned items maintained under dual control?
75. Are working supplies kept to a reasonable minimum, i.e., two or three days' supply, and adequately protected during banking hours?
*76. Is a memorandum control maintained of consigned items?
77. Are separate accounts with the consignor maintained at each issuing location (branch), if applicable?
*78. Is the working supply put in the vault at night and over weekends or holidays or is it otherwise protected?
79. Are remittances for sales made on a regularly scheduled basis, if not daily?

Conclusion

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

Sale of Uninsured Nondeposit Debt Obligations on Bank Premises

Effective date May 1996

Section 4570.1

INTRODUCTION

State member banks have, at times, engaged in issuing nondeposit debt securities on their own behalf or assisted in the sale of these instruments (for example, commercial paper or other short-term or long-term debt securities, such as thrift notes and subordinated debentures) on behalf of their parent bank holding companies or other affiliates. It is important to ensure that these securities are not issued, marketed, or sold in a manner that could give the purchaser the impression that the obligations are federally insured deposits. Consequently, state member banks and their subsidiaries that have issued or plan to issue nondeposit debt securities should not market or sell these instruments in any public area of the bank where retail deposits are accepted, including any lobby area of the bank.

PROCEDURES

This policy is not intended to prevent banks from selling their uninsured debt instruments in a manner that is consistent with sound and prudent banking practices. These instruments generally may be sold to investors in various ways away from the retail deposit-taking and general lobby areas of the bank. In this regard, personnel not regularly involved in deposit-taking activities or in opening new deposit accounts may make prospective investors in the community aware of uninsured debt obligations outside of the retail deposit-taking and general lobby areas. Also, these instruments may generally be sold by an employee or officer segregated from the retail deposit-taking and general lobby areas of the bank, even if the employee or officer occasionally accepts deposits or opens an account (but not as a part of his or her regular duties), so long as the arrangement is not structured in a way that misleads the purchaser or is otherwise contrary to supervisory guidelines.

Further, state member banks involved in this activity should establish procedures to ensure that potential purchasers understand that the debt security is not federally insured or guaranteed. Specifically, the debt security should boldly state on its face that it is not insured by the Federal Deposit Insurance Corporation. In addition, this information should be verbally stated to the purchaser, and, in cases where purchasers do not take physical possession of the obligation, the purchaser should be provided with printed advice that conveys this information.

SUPERVISORY GUIDANCE

As noted, a state member bank may also become involved in the sale of uninsured debt obligations of its parent bank holding company or a nonbank affiliate. It is a longstanding policy of the Federal Reserve that debt obligations of a bank holding company or a nonbank affiliate not be issued, marketed, or sold in a way that conveys the misimpression or misunderstanding that these instruments are either (1) federally insured deposits or (2) obligations of or guaranteed by the subsidiary bank. The purchase of these holding company obligations by retail depositors of the subsidiary bank can, in the event of default, result in losses to individuals who believed that they had acquired federally insured or guaranteed instruments. In addition to the problems created for these individuals, this situation could impair public confidence in the bank and lead to unexpected withdrawals or liquidity pressures.

If a state member bank intends to market or sell or to allow its parent holding company or a nonbank affiliate to market or sell uninsured nondeposit debt obligations on bank premises, the bank should establish internal controls to ensure that the promotion, sale, and subsequent customer relationship resulting from the sale of these debt obligations is separated from the retail deposit-taking functions of the bank. For further information on commercial paper, see section 2030, “Bank Dealer Activities.”

Sale of Uninsured Nondeposit Debt Obligations on Bank Premises

Examination Objectives

Effective date May 1996

Section 4570.2

1. To determine if uninsured nondeposit debt obligations of the state member bank or an affiliate are sold on bank premises.
2. To determine if the policies, practices, procedures, and internal controls for the sale of uninsured nondeposit debt instruments are adequate.
3. To ensure that the marketing and sale of uninsured nondeposit debt instruments are not conducted in a manner that conveys the impression or suggestion that they are federally insured deposits. Additionally, holding company or affiliate instruments should not convey the impression or suggestion that they are obligations of or guaranteed by the state member bank.
4. To ensure that the marketing and sale of uninsured nondeposit debt obligations are sufficiently separated and distinguished from retail banking operations, particularly the deposit-taking function.
5. To initiate corrective action if policies, practices, or procedures related to the sale of uninsured nondeposit debt instruments are deficient.

Sale of Uninsured Nondeposit Debt Obligations on Bank Premises

Examination Procedures

Effective date September 1992

Section 4570.3

1. Verify that the bank does not sell uninsured nondeposit debt instruments at teller windows or other areas where retail deposits are routinely accepted, including general lobby areas surrounding teller windows and personal banking desks.
2. Assess the adequacy of disclosures and the separation of the marketing and sale of uninsured nondeposit debt obligations from the retail deposit-taking function by assuring that:
   a. the debt instrument, advertising, and all related documents disclose prominently in bold print that the debt instrument is not insured by the Federal Deposit Insurance Corporation (bank holding company debt instruments should also state that the instrument is not an obligation of, or guaranteed by, the bank);
   b. advertisements that promote uninsured debt obligations of the bank (or an affiliate) do not also promote insured deposits of the bank in a way that could lead to confusion;
   c. the obligor of the uninsured debt instrument is prominently disclosed and names or logos of the bank are not used on holding company or nonbank affiliate instruments in a way that might suggest the insured bank is the obligor;
   d. adequate verbal disclosures are made during telemarketing contacts and at the time of sale (a review of employee instructions or a telemarketing script, or appropriate questions directed to an employee handling this function, could assist an examiner in assessing the adequacy of verbal disclosure);
   e. retail deposit-taking employees of the insured depository institution are not engaged in the promotion or sale of uninsured nondeposit debt instruments;
   f. information on uninsured nondeposit debt instruments is not contained in the retail deposit statements of customers or in the immediate retail deposit-taking area; and
   g. account information on holdings of uninsured nondeposit debt instruments is not included on insured deposit statements.
3. Encourage the bank to obtain a signed statement from the customer indicating that the customer understands that the uninsured debt instrument is not a deposit and is not FDIC insured.

Depository institutions have become increasingly involved in selling uninsured nondeposit investment products, such as mutual funds or annuities, on their premises to retail customers. In response to this development, an interagency statement on retail sales of nondeposit investment products (interagency statement) was issued on February 15, 1994, to enhance customer protection and lessen possible customer confusion that these products are insured deposits.[1] The interagency statement applies to all insured banks and thrifts, including state member banks and the U.S. branches and agencies of foreign banks.

The guidelines contained in the interagency statement apply to retail recommendations or sales of nondeposit investment products made by—

- employees of a depository institution,
- employees of an affiliated or unaffiliated third party occurring on the premises of the banking organization (including telephone sales, investment recommendations by employees, and sales or recommendations initiated by mail from its premises), and
- sales resulting from a referral of retail customers by the institution to a third party when the depository institution receives a benefit for the referral.

Retail sales include (but are not limited to) sales to individuals by depository-institution personnel or third-party personnel conducted in or adjacent to a depository institution's lobby area. The sales of government and municipal securities made in a depository institution's dealer department located away from the lobby area are not subject to the interagency statement. In addition, the interagency statement generally does not apply to fiduciary accounts administered by a depository institution. However, for fiduciary accounts where the customer directs investments, such as self-directed individual retirement accounts, the disclosures prescribed by the interagency statement (see the "Disclosures and Advertising" subsection below) should be provided. Furthermore, the interagency statement applies to affiliated broker-dealers when the sales occur on the premises of the depository institution. The interagency statement also applies to sales activities of an affiliated broker-dealer resulting from a referral of retail customers by the depository institution.

The Rules of Fair Practice of the Financial Industry Regulatory Authority govern sales of securities by its member broker-dealers. In addition, the federal securities laws prohibit materially misleading or inaccurate representations in connection with the offer or sale of securities and require that sales of registered securities be accompanied by a prospectus that complies with SEC disclosure requirements.

Examiners should determine whether the institution has adequate policies and procedures to govern the conduct of the sales activities on bank premises and, in particular, whether sales of nondeposit investment products are distinguished from the deposit-taking activities of the bank through disclosure and physical means that are designed to prevent customer confusion.

Although the interagency statement does not apply to sales of nondeposit investment products to nonretail customers, such as fiduciary customers, examiners should also apply the examination procedures prescribed in SR-94-34 ("Examination Procedures for Retail Sales of Nondeposit Investment Products," May 26, 1994) when retail customers are directed to the institution's trust department, where they may purchase nondeposit investment products by simply completing a customer agreement.

PROGRAM MANAGEMENT

Banks must adopt policies and procedures governing nondeposit investment product retail sales programs. These policies and procedures should be in place before the commencement of the retail sale of nondeposit investment products on bank premises.

The bank's board of directors is responsible for ensuring that retail sales of nondeposit investment products comply with the interagency statement and with all applicable state and federal laws and regulations. Therefore, the

1. The interagency statement was issued to Federal Reserve Banks under cover of a supervisory letter, SR-94-11 ("Interagency Statement on Retail Sales of Nondeposit Investment Products," February 17, 1994). Additional guidance is provided in SR-95-46 ("Interpretation of Interagency Statement on Retail Sales of Nondeposit Investment Products," September 14, 1995).

board, or a designated committee of the board, should adopt written policies that address the risks and management of these sales programs. Policies and procedures should reflect the size, complexity, and volume of the institution's activities or, when applicable, the institution's arrangements with any third parties selling these products on bank premises. The bank's policies and procedures should be reviewed periodically by the board of directors, or its designated committee, to ensure that they are consistent with the institution's current practices, applicable laws, regulations, and guidelines.

A bank's policies and procedures for nondeposit investment products should, at a minimum, address (1) disclosure and advertising, (2) the physical separation of investment sales from deposit-taking activities, (3) compliance and audit requirements, (4) suitability concerns, and (5) other sales practices and related risks. In addition, policies and procedures should address the following areas.

Types of Products Sold

When evaluating nondeposit investment products, management should consider what products best meet the needs of the bank's customers. Policies should outline the criteria and procedures that will be used to select and periodically review nondeposit investment products that are recommended or sold on the bank's premises. Institutions should periodically review the products offered to ensure that they meet their customers' needs.

Use of Identical or Similar Names

Because of the possibility of customer confusion, a nondeposit investment product must not have a name that is identical to the name of the bank or its affiliates. However, a bank may sell a nondeposit investment product with a similar name as long as the sales program addresses the even greater risk that customers may regard the product as an insured deposit or other obligation of the bank. Moreover, the bank should review the issuer's disclosure documents for compliance with SEC requirements, which call for a thorough explanation of the relationship between the bank and the mutual fund.

The Federal Reserve applies a stricter rule to investment adviser activities under Regulation Y (12 CFR 225.125) when a bank holding company (as opposed to a bank) or nonbank subsidiary acts as an investment advisor to a mutual fund. In this case, the fund may not have a name that is identical to, similar to, or a variation of the name of the bank holding company.

Permissible Use of Customer Information

Banks should adopt policies and procedures on the use of confidential customer information for any purpose in connection with the sale of nondeposit investment products. The industry guidelines permit institutions to share with third parties only limited customer information, such as the name, address, telephone number, and types of products owned. The guidelines do not permit the sharing of more confidential information, such as specific or aggregate dollar amounts of investments or net worth, without the customer's prior acknowledgment and written consent.

Arrangements with Third Parties

A majority of all nondeposit investment products sold on bank premises are sold by representatives of third parties. Under these arrangements, the third party has access to the institution's customers, and the bank is able to make nondeposit investment products available to interested customers without having to commit the resources and personnel necessary to sell the products directly. Third parties include wholly owned subsidiaries of a bank, bank-affiliated broker-dealers (section 20 companies[2] or discount brokerage firms), unaffiliated broker-dealers, insurance companies, or other companies in the business of distributing nondeposit investment products on a retail basis.

Bank management should conduct a comprehensive review of an unaffiliated third party before entering into any arrangement. The review should include an assessment of the third party's

2. A nonbank subsidiary of a bank holding company that has been authorized to underwrite and deal in certain debt and equity securities that cannot be underwritten or dealt in by member banks directly.

financial status, management experience, and ability to fulfill its contractual obligations to the bank.

Banks should enter into written agreements with any affiliated and unaffiliated third parties that sell nondeposit investment products on bank premises. These agreements should be approved by the bank's board of directors or its designated committee. Agreements should outline the duties and responsibilities of each party; describe third-party activities permitted on the institution's premises; address the sharing or use of confidential customer information for investment sales activities; and define the terms for use of the bank's office space, equipment, and personnel. If an arrangement includes dual employees (bank employees also utilized by a third party), the agreement must provide for written employment contracts that specify the duties of these employees and their compensation arrangements.

In addition, a third-party agreement should specify that the third party will comply with all applicable laws and regulations and will conduct its activities in a manner consistent with the interagency statement. The agreement should authorize the institution to monitor the third party's compliance with its agreement, as well as authorize the bank and Federal Reserve examination staff to have access to third-party records considered necessary to evaluate this compliance. These records should include examination results, sales practice reviews, and related correspondence provided to the third party by securities regulatory authorities. Finally, the agreement should provide for indemnification of the institution by an unaffiliated third party for the conduct of its employees in connection with its sales activities. Notwithstanding the provisions of a third-party agreement, bank management should monitor the conduct of nondeposit investment product sales programs to ensure that sales of the products are distinct from other bank activities and are not conducted in a manner that could confuse customers about the lack of insurance coverage for these investments.

Contingency Planning

Nondeposit investment products are subject to price fluctuations caused by changes in interest rates and stock market valuations. In the event of a sudden, sharp drop in the market value of nondeposit investment products, institutions may experience a heavy volume of customer inquiries, complaints, and redemptions. Therefore, management should develop contingency plans to address these situations. A major element of any contingency plan should be to provide customers with access to information about their investments. Other factors to consider in contingency planning include public relations and the ability of operations staff to handle increased volumes of transactions.

DISCLOSURES AND ADVERTISING

Content, Form, and Timing of Disclosures

Nondeposit investment product sales programs should ensure that customers are clearly and fully informed of the nature and risks associated with these products. In addition, nondeposit investment products must be clearly differentiated from insured deposits. The interagency statement identifies the following minimum disclosures that must be made to customers when providing investment advice, making investment recommendations, or effecting nondeposit investment product transactions:

- They are not insured by the FDIC.
- They are not deposits or other obligations of the institution and are not guaranteed by the institution.
- They are subject to investment risks, including the possible loss of the principal invested.

There are limited situations in which the disclosure guidelines need not apply or where a shorter logo format may be used in lieu of the longer written disclosures.

The interagency statement disclosures do not need to be provided in the following situations:

- radio broadcasts of 30 seconds or less;
- electronic signs,[3] and
- signs, such as banners and posters, when they are used only as location indicators.

3. "Electronic signs" may include billboard-type signs that are electronic, time-and-temperature signs, and ticker-tape signs. Electronic signs would not include such media as television, on-line services, or ATMs.

Additionally, third-party vendors not affiliated with the depository institution need not make the interagency statement disclosures on nondeposit investment product confirmations and in account statements that may incidentally, with a valid business purpose, contain the name of the depository institution.

Shorter, logo-format disclosures may be used in visual media, such as television broadcasts, ATM screens, billboards, signs, posters, and written advertisements and promotional materials, such as brochures. The text of an acceptable logo-format disclosure would include the following statements:

- Not FDIC-Insured.
- No Bank Guarantee.
- May Lose Value.

Disclosure is the most important way of ensuring that the differences between nondeposit investment products and insured deposits are understood by retail customers. Accordingly, it is critical that the minimum disclosures be presented clearly and concisely in both oral and written communications. In this regard, the minimum disclosures should be provided—

- orally during any sales presentations (including telemarketing contacts) or when investment advice is given,
- orally and in writing before or at the time an investment account to purchase these products is opened, and
- in all advertisements and other promotional materials (discussed further below).

The minimum disclosures may be made on a customer account agreement or on a separate disclosure form. The disclosures must be conspicuous (highlighted through bolding, boxes, and/or a larger typeface). Disclosures contained directly on a customer account agreement should be located on the front of the agreement or adjacent to the customer signature block.

Banks are to obtain a written acknowledgment—on the customer account agreement or on a separate form—from a customer confirming that he or she has received and understands the minimum disclosures. For nondeposit investment product accounts established before the issuance of the interagency statement, banks should obtain a disclosure acknowledgment from the customer at the time of the customer's next purchase transaction. If an institution solicits customers by telephone or mail, it should ensure that the customers receive the written disclosures and an acknowledgment to be signed and returned to the institution.

Customer account statements, including combined statements for linked accounts and trade confirmations that are provided by the bank or an affiliate, should contain the minimum disclosures if they display the name or logo of the bank or its affiliate. Statements that provide account information about insured deposits and nondeposit investment products should clearly segregate the information about nondeposit investment products from the information about deposits to avoid customer confusion.

Advertising

The interagency statement provides that advertisements in all media forms that identify specific investment products must conspicuously include the minimum disclosures and must not suggest or convey any inaccurate or misleading impressions about the nature of a nondeposit investment product. Promotional material that contains information about both FDIC-insured products and nondeposit investment products should clearly segregate the information about the two product types. When promotional sales materials related to nondeposit investment products are displayed in the bank's retail areas, they should be grouped separately from material related to insured bank products.

Telemarketing scripts should be reviewed to determine whether bank personnel are inquiring about customer investment objectives, offering investment advice, or identifying particular investment products or types of products. In these cases, the scripts must contain the minimum disclosures, and bank personnel relying on the scripts must be formally authorized to sell nondeposit investment products by their employers. Further, these personnel must have training that is the substantive equivalent of that required for personnel qualified to sell securities as registered representatives (see the "Training" subsection below).

Additional Disclosures

A bank should apprise customers of certain material relationships. For example, a customer

should be informed by sales personnel orally and in writing before the sale about any advisory relationship existing between the bank (or an affiliate) and a mutual fund whose shares are being sold by the institution. Similarly, fees, penalties, or surrender charges associated with a nondeposit investment product should be disclosed by sales personnel orally and in writing before or at the time the customer purchases the product. The SEC requires written disclosure of this information in the investment product's prospectus.

If sales activities include any written or oral representations concerning insurance coverage by any entity other than the FDIC (for example, SIPC insurance of broker-dealer accounts, a state insurance fund, or a private insurance company), then clear and accurate explanations of the coverage must also be provided to customers at that time to minimize possible confusion with FDIC insurance. These disclosures should not suggest that other forms of insurance are the substantive equivalent to FDIC deposit insurance.

SETTING AND CIRCUMSTANCES

Physical Separation from Deposit Activities

Selling or recommending nondeposit investment products on bank premises may give the impression that the products are FDIC-insured or are obligations of the bank. To minimize customer confusion with deposit products, nondeposit investment product sales activities should be conducted in a location that is physically distinct from the areas where retail deposits are taken. Bank employees located at teller windows may not provide investment advice, recommend investment products, or accept orders (even unsolicited orders) for nondeposit investment products.

To decide whether nondeposit investment product sales activities are sufficiently separate from deposit activities, the particular circumstances of each bank need to be evaluated. FDIC insurance signs and insured deposit-related promotional material should be removed from the investment product sales area and replaced with appropriate signs indicating that the area is used for the sale of investment products. Signs referring to specific investments should prominently contain the minimum disclosures. In the limited situation where physical constraints prevent nondeposit investment product sales activities from being conducted in a distinct and separate area, the institution has a heightened responsibility to ensure that appropriate measures are taken to minimize customer confusion.

In the case of banks that are affiliated with section 20 companies that sell retail investment products directly to bank customers, the requirement for separation of deposit-taking facilities from the securities operations of the section 20 company is absolute under the relevant firewall conditions imposed on these companies by the Board. Accordingly, retail sales activities conducted by a section 20 company must be in a separate office which, at a minimum, is set off from deposit-taking activities by partitions and identified by signs with the name of the section 20 company. Further, section 20 company employees may not be dual employees of the bank. Business cards for designated sales personnel should clearly indicate that they sell nondeposit investment products or, if applicable, are employed by a broker-dealer.

The interagency statement was intended generally to cover sales made to retail customers in the bank lobby. However, some institutions may have an arrangement whereby retail customers purchase nondeposit investment products at a location of the institution that is generally confined to institutional services (for example, corporate money desk). In these cases, the bank should still ensure that retail customers receive the minimum disclosures to minimize any possible customer confusion with nondeposit investment products and insured deposits.

Hybrid Instruments and Accounts

When an institution offers accounts that link traditional bank deposits with nondeposit investment products, such as a cash-management account,[4] the accounts should be opened in the investment sales area by trained personnel. In light of the hybrid characteristics of these products, the opportunity for customer confusion is amplified, and the institution should take special care during the account-opening process to ensure that a customer is accurately informed that

4. A hybrid account may incorporate deposit and brokerage services, credit/debit card features, and automated sweep arrangements.

- funds deposited into a sweep account will only be FDIC-insured until they are swept into a nondeposit investment product account and
- customer account statements may disclose balances for both insured and nondeposit product accounts.

DESIGNATION, TRAINING, AND SUPERVISION OF PERSONNEL

Hiring and Training of Sales Personnel

Banks hiring sales personnel for nondeposit investment product programs should investigate the backgrounds of prospective employees. When a candidate for employment has previous investment industry experience, the bank should check whether the individual has been the subject of any disciplinary actions by securities, state, or other regulators.

Unregistered bank sales personnel should receive training that is the substantive equivalent of that provided to personnel qualified to sell securities as registered representatives. Training should cover the areas of product knowledge, trading practices, regulatory requirements and restrictions, and customer-protection issues. In addition, training programs should cover the bank's policies and procedures for sales of nondeposit investment products and should be conducted continually to ensure that staff are familiar with new products and compliance issues.

For those bank employees whose sales activities are limited to mutual funds or variable annuities, the equivalent training is that ordinarily needed to pass NASD's series 6 limited representative examination, which typically involves approximately 30 to 60 hours of preparation, including about 20 hours of classroom training. Bank employees who are authorized to sell additional investment products and securities should receive training that is appropriate to pass the NYSE's series 7 general securities representative examination, which typically involves 160 to 250 hours of study, including at least 40 hours of classroom training.

The training of third-party or dual employees is the responsibility of the third party. When entering into an agreement with a third party, bank management should be satisfied that the third party is able to train third-party and dual employees with respect to compliance with the minimum disclosures and other requirements of the interagency statement. Copies of third-party training and compliance materials should be obtained and reviewed by the bank to monitor the third party's performance regarding its training obligations.

Training of Bank Personnel Who Make Referrals

Bank employees, such as tellers and platform personnel, who are not authorized to provide investment advice, make investment recommendations, or sell nondeposit investment products, but who may refer customers to authorized nondeposit investment products sales personnel, should receive training about the strict limitations on their activities. In general, bank personnel who are not authorized to sell nondeposit investment products are not permitted to discuss general or specific investment products, prequalify prospective customers as to financial status and investment history and objectives, open new accounts, or take orders on a solicited or unsolicited basis. These personnel may contact customers for the purposes of—

- determining whether the customer wishes to receive investment information
- inquiring whether the customer wishes to discuss investments with an authorized sales representative, and
- arranging appointments to meet with authorized bank sales personnel or third-party broker-dealer registered sales personnel.

The minimum disclosure guidelines do not apply to referrals made by personnel not authorized to sell nondeposit investment products if the referral does not provide investment advice, identify specific investment products, or make investment recommendations.

Supervision of Personnel

Bank policies and procedures should designate, by title or name, the individuals responsible for supervising nondeposit investment product sales activities, as well as the referral activities of bank employees not authorized to sell these products. Personnel responsible for managing

the sales programs for these products should have supervisory experience and training equivalent to that required of a general securities principal, as required by the NASD for broker-dealers. Supervisory personnel should be responsible for the bank's compliance with policies and procedures on nondeposit investment products, applicable laws and regulations, and the interagency statement. When sales of these products are conducted by a third party, supervisory personnel should be responsible for monitoring compliance with the agreement between the bank and the third party, as well as compliance with the interagency statement, particularly the guideline calling for nondeposit investment product sales to be separate and distinct from the deposit activities of the bank.

SUITABILITY AND SALES PRACTICES

Suitability of Recommendations

Suitability refers to the matching of customer financial means and investment objectives with a suitable product. Placing customers into unsuitable investments could pose consumer compliance and other legal risks. Many first-time investors may not fully understand the risks associated with nondeposit investment products and may assume that the bank is responsible for the preservation of the principal of their investment.

Banks that sell nondeposit investment products directly to customers should develop detailed policies and procedures addressing the suitability of investment recommendations and related recordkeeping requirements. Sales personnel that recommend nondeposit investment products to customers should have reasonable grounds for believing that the recommended products are suitable for the particular customer on the basis of information he or she has provided. A reasonable effort must be made to obtain, record, and update information concerning the customer's financial profile (for example, tax status, other investments, income), investment objectives, and other information necessary to make recommendations.

In determining whether sales personnel are meeting their suitability responsibilities, examiners should review the practices for conformance with the bank's policies and procedures. The examiner's review should include a sample of customer files to determine the extent of customer information collected, recorded, and updated (for subsequent purchases) and should determine whether investment recommendations appear unsuitable in light of this information.

Nondeposit investment product sales programs conducted by third-party broker-dealers are subject to the NASD's suitability and other sales practice rules. To avoid duplicating NASD examination efforts, examiners should rely on the NASD's most recent sales practice review of the third party, when available. If an NASD review has not been completed within the last two years, Reserve Banks should consult with Board staff to determine an appropriate examination scope for suitability compliance before proceeding further.

Sales Practices and Customer Complaints

Banks should have policies and procedures that address undesirable practices by sales personnel, such as practices to generate additional commission income for the employee by churning or switching accounts from one product to another. Banks should have policies and procedures for handling customer complaints related to nondeposit investment products. The process should provide for the recording and tracking of all complaints and require periodic reviews of complaints by compliance personnel. The merits and circumstances of each complaint (including all documentation relating to the transaction) should be considered when determining the proper form of resolution. Reasonable timeframes should be established for addressing complaints.

COMPENSATION

Incentive compensation programs specifically related to the sale of nondeposit investment products may include sales commissions, limited fees for referring prospective customers to an authorized sales representative, and nonmonetary compensation (prizes, awards, and gifts). Compensation that is paid by unaffiliated third parties (for example, mutual fund distributors) to bank staff must be approved in writing by bank management, be consistent with the bank's

written internal code of conduct for the acceptance of remuneration from third parties, and be consistent with the proscriptions of the Bank Bribery Act (18 USC 215) and the banking agencies' implementing guidelines to that act. Compensation policies should establish appropriate limits on the extent of compensation that may be paid to banking organization staff by unaffiliated third parties.

Incentive compensation programs must not be structured in such a way that they result in unsuitable investment recommendations or sales to customers. In addition, if sales personnel sell both deposit and nondeposit products, similar financial incentives should be in place for sales of both types of products. A compensation program that offers significantly higher remuneration for selling a specific product (such as a proprietary mutual fund) may be inappropriate if it results in unsuitable recommendations to customers. A compensation program that is intended to provide remuneration for a group of bank employees (such as a branch or department) is permissible as long as the program is based on the group's overall performance in meeting bank objectives for a broad variety of bank services and products and not on the volume of sales of nondeposit investment products.

Individual bank employees, such as tellers, may receive a one-time nominal fee of a fixed-dollar amount for referring customers to authorized sales personnel to discuss nondeposit investment products. However, the payment of the fee should not depend on whether the referral results in a transaction. Nonmonetary compensation to bank employees for referrals should be similarly structured. Auditors and compliance personnel should not participate in incentive compensation programs that are directly related to the results of nondeposit investment product sales programs.

COMPLIANCE

Banks must develop and maintain written policies and procedures that effectively monitor and assess compliance with the interagency statement and other applicable laws and regulations and that ensure appropriate follow-up to correct identified deficiencies. Compliance programs should be independent of sales activities with respect to scheduling, compensation, and performance evaluations. Compliance findings should periodically be reported to the bank's board of directors or a designated committee of the board as part of the institution's ongoing oversight of nondeposit investment product activities. Compliance personnel should have appropriate training and experience with nondeposit investment product sales programs, applicable laws and regulations, and the interagency statement.

Banks should institute compliance programs for nondeposit investment products that are similar to those of securities broker-dealers. This includes a review of new accounts and a periodic review of transactions in existing accounts to identify any potentially abusive practices, such as unsuitable recommendations, churning, or switching. Compliance personnel should also oversee the prompt resolution of customer complaints and review complaint logs for questionable sales practices. Management-information-system reports on early redemptions and sales patterns for specific sales representatives and products should also be used by compliance personnel to identify any potentially abusive practices. In addition, the referral activities of bank personnel should be reviewed to ensure that they conform to the guidelines in the interagency statement.

When nondeposit investment products are sold by third parties on bank premises, the bank's compliance program should provide for oversight of the third party's compliance with its agreement with the bank, including its conformance to the disclosure and separate-facilities guidelines of the interagency statement. The results of this oversight should be reported to the board of directors or a designated committee of the board. Management should obtain the third party's commitment to promptly correct identified problems. Proper follow-up by the bank's compliance personnel should verify the third party's corrective actions.

AUDITS

Audit personnel should be responsible for assessing the effectiveness of the institution's compliance function and overall management of the nondeposit investment product sales program. The scope and frequency of audit reviews of nondeposit investment product activities will depend on the complexity and sales volume of a sales program and on whether there are any indications of potential or actual problems.

Audits should cover all of the issues discussed in the interagency statement. Internal audit staff should be familiar with nondeposit investment products and receive ongoing training. Findings should be reported to the board of directors or to a designated committee of the board, and proper follow-up should be performed. Audit activities with respect to third parties should include a review of their compliance function and the effectiveness of the bank's oversight of the third party's activities.

1. To determine that the banking organization has taken appropriate measures to ensure that retail customers clearly understand the differences between insured deposits and nondeposit investment products and that they receive the minimum disclosures both orally during sales presentations (including telemarketing) and in writing.
2. To assess the adequacy of the institution's policies and procedures, sales practices, and oversight by management and the board of directors to ensure an operating environment that fosters customer protection in all facets of the sales program.
3. To ensure that the sales program is conducted in a safe and sound manner that is in compliance with the interagency statement, Federal Reserve guidelines, regulations, and applicable laws.
4. To assess the effectiveness of the institution's compliance and audit programs for nondeposit investment product operations.
5. To obtain commitments for corrective action when policies, procedures, practices, or management oversight is deficient or when the institution has failed to comply with the interagency statement or applicable laws and regulations.

1. Verify through the minutes of the board of directors that the directors have approved the sale of uninsured annuities, reviewed, and approved the choice of an underwriter in the past year.
2. Determine if the bank adequately evaluates the underwriter's financial condition at least annually and regularly reviews the credit ratings assigned to the underwriter by at least two independent agencies evaluating annuity underwriters. (Banks engaged in the sale of annuities are expected to sell only products of financially secure underwriters and to make current ratings of the underwriter available to an investor when purchasing an uninsured annuity.)
3. Verify that the bank does not sell uninsured annuities at teller windows or other areas where retail deposits are routinely accepted.
4. Assess the adequacy of disclosures and the separation of the marketing and sale of uninsured annuities from the retail deposit-taking function by ensuring that—
   a. the contract, advertising, and all related documents disclose prominently in bold print that the annuities are not deposits or obligations of an insured depository institution and are not insured by the Federal Deposit Insurance Corporation;
   b. advertisements do not contain words, such as "deposit," "CD," etc., that could lead an investor to believe an annuity is an insured deposit instrument;
   c. the obligor of the annuity contract is prominently disclosed and names or logos of the insured bank are not used in a way that might suggest the insured bank is the obligor;
   d. adequate verbal disclosures are made during telemarketing contacts and at the time of sale;
   e. retail deposit-taking employees of the insured depository institution are not engaged in the promotion or sale of uninsured annuities;
   f. information on uninsured annuities is not contained in retail deposit statements of customers (either as advertising on deposit statements or as "junk mail" stuffers included with deposit statements) or in the immediate retail deposit-taking area;
   g. account information on annuities owned by customers is not included on insured deposit statements; and
   h. officer or employee remuneration associated with selling annuities is limited to reasonable levels in relation to the individual's salary. (As a guideline in reviewing remuneration, see the Board's policy statement on disposition of credit life insurance, as discussed in the Consumer Credit, Examination Procedures, section of this manual.)
5. If the bank allows a third-party entity to market annuities on depository-institution premises, assess the adequacy of disclosures and the separation of the marketing and sale of uninsured annuities from the retail deposit-taking function by determining that—
   a. the bank has ensured that the third-party company is properly registered or licensed to conduct this activity,
   b. bank personnel are not involved in sales activities conducted by the third party,
   c. desks or offices used to market or sell annuities are separate and distinctly identified as being used by an outside party, and
   d. bank personnel do not normally use desks or offices used by a third party for annuities sales.
6. Encourage the bank to obtain a signed statement from the customer indicating that the customer understands that the annuity is not a deposit or any other obligation of the bank, that the bank is only acting as an agent for the insurance company (underwriter), and that the annuity is not FDIC-insured.