EXAMINATION AND SUPERVISORY AUTHORITY AND CONFIDENTIALITY PROVISIONS

The Federal Reserve System's statutory examination authority permits examiners to review all books and records maintained by a financial institution that is subject to the Federal Reserve's supervision. This authority extends to all documents.[1] Section 11(a)(1) of the Federal Reserve Act provides that the Board has the authority to examine, at its discretion, the accounts, books, and affairs of each member bank and to require such statements and reports as it may deem necessary.

Federal Reserve supervisory staff (includes the examination staff), therefore, may review *all* books and records of a banking organization that is subject to Federal Reserve supervision.[1a] In addition, under the Board's Rules Regarding the Availability of Information, banking organizations are prohibited from disclosing confidential supervisory information without prior written permission of the Board's General Counsel.[1b] Confidential supervisory information is defined to include any information related to the examination of a banking organization.[1c] Board staff have taken the position that identification of information requested by, or provided to, supervisory staff—including the fact that an examination has taken or will take place—is related to an examination and falls within the definition of confidential supervisory information. It is contrary to Federal Reserve regulation and policy for agreements to contain confidentiality provisions that (1) restrict the banking organization from providing information to Federal Reserve supervisory staff;[1] (2) require or permit, without the prior approval of the Federal Reserve, the banking organization to disclose to a counterparty that any information will be or was provided to Federal Reserve supervisory staff; or (3) require or permit, without the prior approval of the Federal Reserve, the banking organization to inform a counterparty of a current or upcoming Federal Reserve examination or any nonpublic Federal Reserve supervisory initiative or action. Banking organizations that have entered into agreements containing such confidentiality provisions are subject to legal risk. (See SR- 07-19.)

EXAMINATION-FREQUENCY GUIDELINES FOR STATE MEMBER BANKS

The Federal Reserve is required to conduct a full-scope, on-site examination of every insured member bank at least once during each 12-month period, with the exception that certain small institutions can be examined once during each 18-month period. The 18-month examination period can be applied to those banks that—

- have total assets of less than $500 million;[1d]
- are well capitalized;
- were assigned a management rating of 1 or 2 by the Federal Reserve as part of the bank's rating under the Uniform Financial Institutions Rating System;
- were assigned a composite CAMELS rating of 1 or 2 by the Federal Reserve at their most recent examination;
- are not subject to a formal enforcement proceeding or action; and
- have not had a change in control during the preceding 12-month period in which a full-scope, on-site examination would have been required but for the above exceptions.

(See section 208.64 of Regulation H and 72 *Fed. Reg.* 17798, April 10, 2007, and 72 *Fed. Reg.* 54347, September 25, 2007.) The exceptions do not limit the authority of the Federal Reserve to examine any insured member bank as frequently as deemed necessary. (See also SR-07-8 and SR-97-8.)

1. SR-97-17 details the procedure supervisory staff should follow if a banking organization declines to provide information asserting a claim of legal privilege.

1a. Supervisory staff include individuals who are on and/or off site.

1b. 12 CFR 261.20(g).

1c. 12 CFR 261.2(c)(1)(i).

1d. Based on jointly issued interim rules (effective April 10, 2007) issued by the Federal Reserve Board (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS). The interim rule was adopted as final, without change, on September 11, 2007. (See 72 *Fed. Reg.* 54347, September 25, 2007.) The interim rules implemented section 605 of the Financial Services Regulatory Relief Act of 2006 (FSRRA) and Public Law 109-473. Previously, the 18-month examination cycle was available only for institutions that had total assets of $250 million or less.

Alternate-Year Examination Program

The frequency of examination may also be affected by the alternate-year examination program. Under the alternate-year examination program, those banks that qualify are examined in alternate examination cycles by the Reserve Bank and the state. Thus, a particular bank would be examined by the Reserve Bank in one examination cycle, the state in the next, and so on. Any bank may be removed from the program and examined at any time by either agency, and either agency can meet with a bank's management or board of directors or initiate supervisory action whenever deemed necessary.

Banks that are ineligible for an alternate-year examination are those institutions that are in excess of $10 billion in assets and are rated a composite 3 or worse. De novo banks are also ineligible until they are rated 1 or 2 for two consecutive examinations after they have commenced operations. Also, a bank that undergoes a change in control must be examined by the Federal Reserve within 12 months of the change in control.

SUPERVISION OF STATE-CHARTERED BANKS

In May 2004, the State-Federal Working Group, an interagency group of state bank commissioners and senior officials from the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC), developed a recommended-practices document designed to reiterate and reaffirm the need for a commonsense approach for collaborating with states in the supervision of state-chartered banking organizations.[2] The recommended practices highlight the importance of communication and coordination between state and federal banking agencies in the planning and execution of supervisory activities.

When communicating and coordinating with other agencies, examination and supervisory staff should follow the common courtesies and recommended practices identified in the May 2004 document. The recommended practices reinforce the long-standing commitment of federal and state banking supervisors to provide efficient, effective, and seamless oversight of state banks of all sizes, whether those institutions operate in a single state or more than one state. The recommended practices also minimize, to the fullest extent possible, the regulatory burden placed on state-chartered banks—thus further supporting and fostering a seamless supervisory process. (See SR-04-12.)

Recommended Practices for State Banking Departments, the FDIC, and the Federal Reserve

1. State and federal banking agencies should take steps to ensure that all staff responsible for the supervision and examination of state-chartered banks are familiar with the principles contained in the agreement. State and federal banking agencies should ensure that adherence to the principles in the agreement is communicated as a priority within their respective agencies at all levels of staff—ranging from the field examiners to the officers in charge of supervision and to state bank commissioners.
2. Home-state supervisors should make every effort to communicate and coordinate with host-state supervisors as an important part of supervising multistate banks as specified in the Nationwide Cooperative Agreement executed by the state banking departments and recognized by the federal agencies in the agreement.
3. State and federal banking agencies should consider inviting one another to participate in regional examiner training programs and/or seminars to discuss emerging issues and challenges observed in the banking industry.
4. Federal and state banking departments should maintain and share current lists of their staff members designated as PCPs (primary contact persons) for their institutions.
5. PCPs and EICs (examiners-in-charge) from the state banking department(s) and federal agencies should discuss and prepare super-

2. The source for the recommended practices is the November 14, 1996, Nationwide State and Federal Supervisory Agreement (the agreement) to enhance the overall state-federal coordinated supervision program for state-chartered banks. The agreement established a set of core principles to promote coordination in the supervision of all interstate banks, with particular emphasis on complex or larger (for example, $1 billion or more of assets) institutions. (See SR-96-33.) These principles are equally applicable and important when supervisors from federal and state banking agencies are communicating and coordinating the supervision of state-chartered banks operating within a single state.

visory plans at least once during the examination cycle, and more frequently as appropriate for institutions of greater size or complexity or that are troubled. The agencies should discuss and communicate changes to the plan as they may evolve over the examination cycle. The supervisory plans should be comprehensive, including examination plans, off-site monitoring, follow-up or target reviews, supervisory actions, etc., as applicable.

6. The PCPs from the home-state banking department and federal banking agencies should make every effort to share reports that their individual agencies have produced through their off-site monitoring program or through targeted supervisory activities.
7. State and federal banking agencies should notify one another as early as possible if their agency cannot conduct a supervisory event (e.g., examination) that was previously agreed upon—or if the agency intends to provide fewer examiners/resources than originally planned.
8. Meetings with bank management and directors should involve both the appropriate staff in the home-state banking department and in the responsible federal banking agency whenever possible. If a joint meeting is not possible or appropriate (for example, the bank arranges the meeting with one agency only), the other agency (the home-state banking department or the responsible federal banking agency as applicable) should be informed of the meeting.
9. The home-state and responsible federal agency should make every effort to issue a joint exam report in the 45-day time frame identified in the agreement. If circumstances prevent adherence to time frames identified in the agreement, the state and federal agencies should coordinate closely and consider benchmarks or timing requirements that may apply to the other agency.
10. All corrective-action plans (for example, memoranda of understanding, cease-and-desist orders) should be jointly discussed, coordinated, and executed to the fullest extent possible among all examination parties involved. Also, all information on the institution's corrective-action plan and progress made toward implementing the plan should be shared.
11. To ensure that messages to management are consistent to the fullest extent possible, supervisory conclusions or proposed actions should only be communicated to bank management, the bank board of directors, or other bank staff after such matters have been fully vetted within and between the federal banking agency and home-state banking department. The vetting process should, to the fullest extent possible, adhere to the exit meeting and examination report issuance time frames specified in the agreement. All parties should make every effort to expedite the process in order to deliver timely exam findings and efficient regulatory oversight.
12. When differences between the agencies arise on important matters, such as examination conclusions or proposed supervisory action, senior management from the home-state banking department and the appropriate federal banking agency should communicate to try to resolve the differences. In the event that the state and federal banking agency cannot reach agreement on important matters affecting the supervised institution, the respective agencies should coordinate the communication of those differences to the management or board of directors of the supervised institution, including the timing thereof and how the differing views will be presented.

EXAMINATION OF INSURED DEPOSITORY INSTITUTIONS BEFORE THEY BECOME OR MERGE INTO STATE MEMBER BANKS

Premembership examinations of state nonmember banks, national banks, and savings associations seeking to convert to state-membership status will not be required if the bank or savings association seeking membership meets the criteria for "eligible bank," as defined in section 208.2(e) of Regulation H.[2a] Additionally,

2a. "Eligible bank" is defined to mean a member bank that (1) is well capitalized; (2) has a composite CAMELS rating of 1 or 2; (3) has a CRA rating of Outstanding or Satisfactory; (4) has a rating of 1 or 2 as of its most recent consumer compliance examination; and (5) has no major unresolved supervisory issues outstanding, as determined by the Board or appropriate Federal Reserve Bank in its discretion. A major unresolved supervisory issue could also arise from significant trust or fiduciary activities that are found to be conducted in a less-than-satisfactory manner.

examinations of state nonmember banks, national banks, and savings associations seeking to merge into a state member bank will not be required so long as the state member bank, on an existing and pro forma basis, meets the criteria for eligible bank.

For those institutions not subject to a premembership or premerger examination, risk assessments and supervisory strategies should be completed no later than 30 days after the conversion or merger. To the extent issues or concerns arise, targeted or, if warranted, full-scope examinations of the converted or merged institution should be conducted as soon as possible after the conversion or merger. For a state member bank that was formerly a savings association or that acquired a savings association, the risk assessment and supervisory strategy should pay particular attention to activities conducted by a service corporation subsidiary that may not be permissible activities for a state member bank.

Premembership or premerger examinations should generally be conducted for an insured depository institution that does not meet the criteria for eligible bank. Consistent with a risk-focused approach, these examinations can be targeted, as appropriate, to the identified area (or areas) of weakness. The Reserve Bank may, in its discretion, waive the examination requirement if it is determined that conducting an examination would be (1) inconsistent with a risk-focused approach or (2) unlikely to provide information that would assist materially in evaluating the statutory and regulatory factors that the Federal Reserve is required to consider in acting on the membership or merger application.[2b] If an examination is waived, the Reserve Bank should prepare and maintain documentation supporting its decision.

In all circumstances, each Reserve Bank is responsible for ensuring that the examination-frequency time frames established by Federal Reserve policy and section 111 of the Federal Deposit Insurance Corporation Improvement Act (FDICIA) are adhered to. When the statutory deadline for an examination of a depository institution seeking membership is approaching or has passed, a Federal Reserve examination of the institution should be conducted as soon as practicable after the institution becomes a state member bank. (See SR-98-28.)

OBJECTIVES OF THE SUPERVISORY PROCESS

The Federal Reserve is committed to ensuring that the supervisory process for all institutions under its purview meets the following objectives:

- *Provides flexible and responsive supervision.* The supervisory process is dynamic and forward-looking, so it responds to technological advances, product innovation, and new risk-management systems and techniques, as well as to changes in the condition of an individual financial institution and to market developments.
- *Fosters consistency, coordination, and communication among the appropriate supervisors.* Seamless supervision, which reduces regulatory burden and duplication, is promoted. The supervisory process uses examiner resources effectively by using the institution's internal and external risk-assessment and -monitoring systems; making appropriate use of joint and alternating examinations; and tailoring supervisory activities to an institution's condition, risk profile, and unique characteristics.
- *Promotes the safety and soundness of financial institutions.* The supervisory process effectively evaluates the safety and soundness of banking institutions, including the assessment of risk-management systems, financial condition, and compliance with laws and regulations.

If a bank has not yet received compliance or CRA ratings from a bank regulatory authority, the Federal Reserve Board will look to the bank's holding company to determine whether the bank's application should receive expedited processing. If the bank's holding company meets the criteria for expedited processing under section 225.14(c) of Regulation Y, the bank's membership or branch application will be eligible for expedited processing. Banks that (1) have not yet received compliance or CRA ratings and (2) either are not owned by a bank holding company or are owned by a bank holding company that does not meet the criteria for expedited processing are not eligible for expedited treatment.

2b. Since membership in the Federal Reserve System does not confer deposit insurance, the membership applications do not include the requirements of the Community Reinvestment Act (CRA). Nevertheless, a less-than-satisfactory CRA rating, especially if it reflects a chronic record of weak CRA performance, would presumably reflect poorly upon the abilities of the institution's management. Consequently, a determination of whether or not to conduct a premembership CRA examination should be based on a risk-focused assessment of the issues involved, with an institution's CRA performance being only one of the factors considered from a risk-focused perspective.

- *Provides a comprehensive assessment of the institution.* The supervisory process integrates specialty areas (for example, information technology systems, trust, capital markets, and consumer compliance) and functional risk assessments and reviews, in cooperation with interested supervisors, into a comprehensive assessment of the institution.

RISK-FOCUSED EXAMINATIONS

Historically, examinations relied significantly on transaction-testing procedures when assessing a bank's condition and verifying its adherence to internal policies, procedures, and controls. In a highly dynamic banking market, however, transaction testing by itself is not sufficient for ensuring the continued safe and sound operation of a banking organization. Evolving financial instruments and markets have enabled banking organizations to rapidly reposition their portfolio risk exposures. Therefore, periodic assessments of the condition of a financial institution that are based on transaction testing alone cannot keep pace with the moment-to-moment changes occurring in financial risk profiles.

To ensure that institutions have in place the processes necessary to identify, measure, monitor, and control risk exposures, examinations have increasingly emphasized evaluating the appropriateness of these processes, evolving away from a high degree of transaction testing. Under a risk-focused examination approach, the degree of transaction testing should be reduced when internal risk-management processes are determined to be adequate or when risks are minimal. However, when risk-management processes or internal controls are considered inappropriate, such as by an inadequate segregation of duties or when on-site testing determines processes to be lacking, additional transaction testing must be performed. Testing should be sufficient to fully assess the degree of risk exposure in a particular function or activity. In addition, if an examiner believes that a banking organization's management is being less than candid, has provided false or misleading information, or has omitted material information, then substantial on-site transaction testing should be performed.

Compliance with Laws and Regulations

Compliance with relevant laws and regulations should be assessed at every examination. The steps taken to complete these assessments will vary depending on the circumstances of the institution subject to review. When an institution has a history of satisfactory compliance with relevant laws and regulations or has an effective compliance function, only a relatively limited degree of transaction testing need be conducted to assess compliance. At institutions with a less satisfactory compliance record or that lack a compliance function, more-extensive review will be necessary.

Changes in the General Character of a Bank's Business

In conjunction with assessing overall compliance with relevant laws and regulations, examiners should review for compliance with the requirements of Regulation H, which sets forth the requirements for membership of state-chartered banks in the Federal Reserve System and imposes certain conditions of membership on applicant banks. Under the regulation, a member bank must "at all times conduct its business and exercise its powers with due regard to safety and soundness" and "may not, without the permission of the Board, cause or permit any change in the general character of its business or in the scope of the corporate powers it exercises at the time of admission to membership." (See SR-02-9 and section 208.3(d)(1) and (2) of Regulation H (12 CFR 208.3(d)(1) and (2)).)

State member banks must receive the prior approval of the Board before making any significant change in business plans. The trend toward more-diverse, more-complex, and, at times, riskier activities at some banks has raised the importance of this prior-approval requirement.

Changes in the general character of a bank's business would include, for example, becoming a primarily Internet-focused or Internet-only operation, or concentrating solely on subprime lending or leasing activities. Depending on how they are conducted and managed, these activities can present novel risks for banking organizations and may also present risks to the deposit insurance fund. In many cases, these activities involve aggressive growth plans and may give

rise to significant financial, managerial, and other supervisory issues.

In applications for membership in the Federal Reserve System, careful consideration is given to a bank's proposed business plan to ensure, at a minimum, that appropriate financial and managerial standards are met. Likewise, the other federal banking agencies consider a bank's business plan when they review applications for federal deposit insurance, in the case of the Federal Deposit Insurance Corporation (FDIC), or applications for a national bank or federal thrift charter, in the case of the Office of the Comptroller of the Currency (OCC) or the Office of Thrift Supervision (OTS). The OCC, the FDIC, and the OTS have been conditioning their approvals of applications on a requirement that, during the first three years of operations, the bank or thrift provides prior notice or obtains prior approval of any proposed significant deviations or changes from its original operating plan. Rather than use similar commitments, the Federal Reserve has relied on the provisions of Regulation H to address situations in which a state member bank proposes to materially change its core business plan.

Federal Reserve supervisors will be monitoring changes in the general character of a state member bank's business as part of the Federal Reserve's normal supervisory process to ensure compliance with the requirements of Regulation H and with safe and sound banking practices. This review should be conducted at least annually by the Reserve Bank. A significant change in a bank's business plan without the Board's prior approval would be considered a violation of Regulation H and would be addressed through follow-up supervisory action.

Branches

When reviewing domestic-branch applications, the guidelines in section 208.6(b) of Regulation H are followed. The Board reviews the financial condition and management of the applying bank, the adequacy of the bank's capital and its future earning prospects, the convenience and needs of the community to be served, CRA and Regulation BB performance for those branches that will be accepting deposits, and whether the bank's investment in premises for the branch is consistent with section 208.21 of Regulation H. A state member bank that desires to establish a new branch facility may be eligible for expedited processing of its application by the Reserve Bank if it is an eligible bank, as defined in section 208.2(e) of Regulation H.

A member bank may also choose to submit an application that encompasses multiple branches that it proposes to establish within one year of the approval date. Unless notification is waived, the bank must notify the appropriate Reserve Bank within 30 days of opening any branch approved under a consolidated application. Although banks are not required to open an approved branch, approvals remain valid for one year. During this period, the Board or the appropriate Reserve Bank may notify the bank that in its judgment, based on reports of condition, examinations, or other information, there has been a change in the bank's condition, financial or otherwise, that warrants reconsideration of the approval. (See Regulation H, section 208.6(d).)

Insured depository institutions that intend to close branches must comply with the requirements detailed in section 42 of the Federal Deposit Insurance Act (the FDI Act) (12 USC 1831r-1). Section 42(e) requires that banks provide 90 days' notice to both customers and, in the case of insured state member banks, the Federal Reserve Board, before the date of the proposed branch closings. The notice must include a detailed statement of the reasons for the decision to close the branch and statistical and other information in support of those stated reasons. A similar notice to customers must be posted in a conspicuous manner on the premises of the branch to be closed, at least 30 days before the proposed closing. There are additional notice, meeting, and consultation requirements for proposed branch closings by interstate banks in low- or moderate-income areas. Finally, the law requires each insured depository institution to adopt policies for branch closings. (See the revised joint policy statement concerning insured depository institutions' branch-closing notices and policies, effective June 29, 1999,[2c] *Federal Reserve Regulatory Service,* 3–1503.5.) Examiners and supervisors need to be mindful of the section 42 statutory requirements and this joint policy.

Section 208.6(f) of Regulation H states that a branch relocation, defined as a movement that

2c. See also 64 *Fed. Reg.* 34844.

occurs within the immediate neighborhood and does not substantially affect the nature of the branch's business or customers served, is not considered a branch closing. Section 208.2(c)(2)(ii) of Regulation H states (in one of six exclusions) that a branch does not include an office of an affiliated or unaffiliated institution that provides services to customers of the member bank on behalf of the member bank, so long as the institution is not "established or operated" by the bank. For example, a bank could contract with an unaffiliated or affiliated institution to receive deposits; cash and issue checks, drafts, and money orders; change money; and receive payments of existing indebtedness without becoming a branch of that bank. The bank could also (1) have no ownership or leasehold interest in the institution's offices, (2) have no employees who work for the institution, and (3) not exercise any authority or control over the institution's employees or methods of operation.

Prohibition on Branches Being Established Primarily for Deposit Production

Section 109 of the Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 (the Interstate Act) (12 USC 1835a) prohibits any bank from establishing or acquiring a branch or branches outside of its home state primarily for the purpose of deposit production. In 1997, the banking agencies published a joint final rule implementing section 109. (See 62 *Fed. Reg.* 47728, September 10, 1997.) Section 106 of the Gramm-Leach-Bliley Act of 1999 expanded the coverage of section 109 of the Interstate Act to include any branch of a bank controlled by an out-of-state bank holding company. On June 6, 2002, the Board and the other banking agencies published an amendment to their joint final rule (effective October 1, 2002) to conform the uniform rule to section 109. (See 67 *Fed. Reg.* 38844.) The amendment expands the regulatory prohibition against interstate branches being used as deposit-production offices to include any bank or branch of a bank controlled by an out-of-state bank holding company, including a bank consisting only of a main office. (See Regulation H, section 208.7(b)(2).)

Minimum Statewide Loan-to-Deposit Ratios

Section 109 sets forth a process to test compliance with the statutory requirements. First, a bank's statewide loan-to-deposit ratio[2d] is compared with the host-state loan-to-deposit ratio[2e] for banks in a particular state. If the bank's statewide loan-to-deposit ratio is at least one-half of the published host-state loan-to-deposit ratio, then it has complied with section 109. A second step is conducted if a bank's statewide loan-to-deposit ratio is less than one-half of the published ratio for that state or if data are not available at the bank to conduct the first step. The second step involves determining whether the bank is reasonably helping to meet the credit needs of the communities served by its interstate branches. If a bank fails both of these steps, it has violated section 109 and is subject to sanctions.

RISK-MANAGEMENT PROCESSES AND INTERNAL CONTROLS

The Federal Reserve has always placed 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, legal, and reputational risk. (See SR-97-24 and SR-97-25.)

- *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

2d. The statewide loan-to-deposit ratio relates to an individual bank and is the ratio of a bank's loans to its deposits in a particular state where the bank has interstate branches.

2e. The host-state loan-to-deposit ratio is the ratio of total loans in a state to total deposits from the state for all banks that have that state as their home state. For state-chartered banks, the home state is the state where the bank was chartered.

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 the potential that the institution 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 a banking organization.
- *Reputational risk* is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.

In practice, an institution's business activities present various combinations and concentrations of these risks, depending on the nature and scope of the particular activity. The following discussion provides guidelines for determining the quality of bank management's formal or informal systems for identifying, measuring, and containing these risks.

Elements of Risk Management

When evaluating the quality of risk management as part of the evaluation of the overall quality of management, examiners should consider 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

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

Active Board and Senior Management Oversight

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

- The board and 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.
- The board has reviewed and approved appropriate policies to limit risks inherent in the institution's lending, investing, trading, trust, fiduciary, and other significant activities or products.
- The board and management are sufficiently familiar with and are using adequate record-keeping and reporting systems to measure and monitor the major sources of risk to the organization.
- The board periodically reviews and approves risk-exposure limits to conform with any changes in the institution's strategies, reviews new products, and reacts to changes in market conditions.
- 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.
- 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.
- 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.
- 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, 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

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 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

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 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

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 reviews the effectiveness of internal audits and other control-review activities regularly.

RISK-FOCUSED SUPERVISION OF COMMUNITY BANKS

Understanding the Bank

The risk-focused supervision process for community banks involves a continuous assessment of the bank, which leads to an understanding of the bank that enables examiners to tailor their examination to the bank's risk profile. In addition to examination reports and correspondence files, each Reserve Bank maintains various surveillance reports that identify outliers when a bank is compared to its peer group. Review of this information helps examiners identify a bank's strengths and vulnerabilities, and is the foundation for determining the examination activities to be conducted.

Contact with the organization is encouraged to improve the examiners' understanding of the institution and the market in which it operates. A pre-examination interview or visit should be conducted as a part of each examination. This meeting gives examiners the opportunity to learn about any changes in bank management and changes to the bank's policies, strategic direction, management information systems, and other activities. During this meeing, particular emphasis should be placed on learning about the bank's new products or new markets it may have entered. The pre-examination interview or visit also provides examiners with (1) management's view of local economic conditions, (2) an understanding of the bank's regulatory compliance practices, and (3) its management information systems and internal and/or external audit function. In addition, Reserve Banks should contact the state banking regulator to determine whether it has any special areas of concern that examiners should focus on.

Reliance on Internal Risk Assessments

As previously discussed in the subsection ''Risk-Management Processes and Internal Controls,'' the entire spectrum of risks facing an institution should be considered when assessing a bank's risk portfolio. Internal audit, loan-review, and compliance functions are integral to a bank's own assessment of its risk profile. If applicable, it may be beneficial to discuss with the bank's external auditor the results of its most recent audit for the bank. Such a discussion gives the examiner the opportunity to review the external auditor's frequency, scope, and reliance on internal audit findings. Examiners should consider the adequacy of these functions in determining the risk profile of the bank, and be alert to opportunities to reduce regulatory burden by testing rather than duplicating the work of internal and external audit functions. See the subsection ''Risk-Focused Examinations'' for a discussion on transaction testing.

Preparation of a Scope Memorandum

An integral product in the risk-focused methodology, the scope memorandum identifies the central objectives of the examination. The memorandum also ensures that the examination strategy is communicated to appropriate examination staff, which is of key importance, as the scope will likely vary from examination to examination. Examination procedures should be tailored to the characteristics of each bank, keeping in mind its size, complexity, and risk profile. Procedures should be completed to the degree necessary to determine whether the bank's management understands and adequately controls the levels and types of risk that are assumed. In addition, the scope memorandum should address the general banking environment, economic conditions, and any changes foreseen by bank management that could affect

the bank's condition. Some of the key factors that should be addressed in the scope memorandum are described below.

Preliminary Risk Assessment

A summary of the risks associated with the bank's activities should be based on a review of all available sources of information on the bank, including, but not limited to, prior examination reports, surveillance reports, correspondence files, and audit reports. The scope memorandum should include a preliminary assessment of the bank's condition and major risk areas that will be evaluated through the examination process. For detailed discussion of risk assessments and risk matrices, see the subsection "Risk-Focused Supervision of Large, Complex Institutions."

Summary of Pre-Examination Meeting

The results of the pre-examination meeting should be summarized. Meeting results that affect examination coverage should be emphasized.

Summary of Audit and Internal Control Environment

A summary of the scope and adequacy of the audit environment should be prepared, which may result in a modification of the examination procedures initially expected to be performed. Activities that receive sufficient coverage by the bank's audit system can be tested through the examination process. Certain examination procedures could be eliminated if their audit and internal control areas are deemed satisfactory.

Summary of Examination Procedures

As discussed below, examination modules have been developed for the significant areas reviewed during an examination. The modules are categorized as primary or supplemental. The primary modules must be included in each examination. However, procedures within the primary modules can be eliminated or enhanced based on the risk assessment or the adequacy of the audit and internal control environment. The scope memorandum should specifically detail the areas within each module to be emphasized during the examination process. In addition, any supplemental modules used should be discussed.

Summary of Loan Review

On the basis of the preliminary risk assessment, the anticipated loan coverage should be detailed in the scope memorandum. In addition to stating the percentage of commercial and commercial real estate loans to be reviewed, the scope memorandum should identify which specialty loan reference modules of the general loan module are to be completed. The memorandum should specify activities within the general loan module to be reviewed as well as the depth of any specialty reviews.

Job Staffing

The staffing for the examination should be detailed. Particular emphasis should be placed on ensuring that appropriate personnel are assigned to the high-risk areas identified in the bank's risk assessment.

Examination Modules

Standardized electronic community bank examination modules have been developed and designed to define common objectives for the review of important activities within institutions and to assist in the documentation of examination work. It is expected that full-scope examinations will use these modules.

The modules establish a three-tiered approach for the review of a bank's activities: The first tier is the core analysis, the second tier is the expanded review, and the final tier is the impact analysis. The core analysis includes a number of decision factors that should be considered collectively, as well as individually, when evaluating the potential risk to the bank. To help the examiner determine whether risks are adequately managed, the core analysis section contains a list of procedures that may be considered for implementation. Once the relevant procedures are performed, the examiner should document conclusions in the core analysis decision factors. When significant deficiencies or weaknesses are noted in the core analysis review, the examiner is required to complete the expanded analysis

for those decision factors that present the greatest degree of risk for the bank. However, if the risks are properly managed, the examiner can conclude the review.

The expanded analysis provides guidance for determining if weaknesses are material to the bank's condition and if they are adequately managed. If the risks are material or inadequately managed, the examiner is directed to perform an impact analysis to assess the financial impact to the bank and whether any enforcement action is necessary.

The use of the modules should be tailored to the characteristics of each bank based on its size, complexity, and risk profile. As a result, the extent to which each module should be completed will vary from bank to bank. The individual procedures presented for each level are meant only to serve as a guide for answering the decision factors. Not every procedure requires an individual response, and not every procedure may be applicable at every community bank. Examiners should continue to use their discretion when excluding any items as unnecessary in their evaluation of decision factors.

RISK-FOCUSED SUPERVISION OF LARGE COMPLEX INSTITUTIONS

The Federal Reserve recognizes a difference in the supervisory requirements for community banks and large complex banking organizations (LCBOs). The complexity of financial products, sophistication of risk-management systems (including audit and internal controls), management structure, and geographic dispersion of operations are but a few of the areas in which large institutions may be distinguished from community banks. While close coordination with state banking departments, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) is important for fostering consistency among banking supervisors and reducing the regulatory burden for community banks, it is critical for large complex banking organizations.

The examination approaches for both large complex institutions and community banks are risk-focused processes that rely on an understanding of the institution, the performance of risk assessments, the development of a supervisory plan, and examination procedures tailored to the risk profile. However, the two approaches are implemented differently: The process for complex institutions relies more heavily on a central point of contact and detailed risk assessments and supervisory plans before the on-site examination or inspection. In comparison, for small or noncomplex institutions and community banks, risk assessments and examination activities may be adequately described in the scope memorandum.

Key Elements

To meet the supervisory objectives discussed previously and to respond to the characteristics of large institutions, the framework for risk-focused supervision of large complex institutions contains the following key elements:

- *Designation of a central point of contact.* Large institutions typically have operations in several jurisdictions, multiple charters, and diverse product lines. Consequently, the supervisory program requires that a "central point of contact" be designated for each institution to facilitate coordination and communication among the numerous regulators and specialty areas.
- *Review of functional activities.* Large institutions are generally structured along business lines or functions, and some activities are managed on a centralized basis. As a result, a single type of risk may cross several legal entities. Therefore, the supervisory program incorporates assessments along functional lines to evaluate risk exposure and its impact on safety and soundness. These functional reviews will be integrated into the risk assessments for specific legal entities and used to support the supervisory ratings for individual legal entities.[3]
- *Focus on risk-management processes.* Large institutions generally have highly developed risk-management systems, such as internal audit, loan review, and compliance. The supervisory program emphasizes each institution's responsibility to be the principal source for detecting and deterring abusive and unsound practices through adequate internal controls and operating procedures. The pro-

3. When functions are located entirely in legal entities that are not primarily supervised by the Federal Reserve, the results of supervisory activities conducted by the primary regulator will be used to the extent possible to avoid duplication of activities.

gram incorporates an approach that focuses on and evaluates the institution's risk-management systems, yet retains transaction testing and supervisory rating systems, such as the CAMELS, bank holding company RFI/C(D), and ROCA rating systems. This diagnostic perspective is more dynamic and forward looking because it provides insight into how effectively an institution is managing its operations and how well it is positioned to meet future business challenges.

- *Tailoring of supervisory activities.* Large institutions are unique, but all possess the ability to quickly change their risk profiles. To deliver effective supervision, the supervisory program incorporates an approach that tailors supervisory activities to the risk profile of an institution. By concentrating on an institution's major risk areas, examiners can achieve a more relevant and penetrating understanding of the institution's condition.
- *Emphasis on ongoing supervision.* Large institutions face a rapidly changing environment. Therefore, the supervisory program emphasizes ongoing supervision through increased planning and off-site monitoring. Ongoing supervision allows for timely adjustments to the supervisory strategy as conditions change within the institution and economy.

Covered Institutions

For purposes of the risk-focused supervision framework, large complex institutions generally have (1) a functional management structure, (2) a broad array of products, (3) operations that span multiple supervisory jurisdictions, and (4) consolidated assets of $1 billion or more.[4] These institutions may be state member banks, bank holding companies (including their nonbank and foreign subsidiaries), and branches and agencies of foreign banking organizations. However, if an institution with consolidated assets totaling $1 billion or more does not have these characteristics, the supervisory process adopted for community banks may be more appropriate. Conversely, the complex-institution process may be appropriate for some organizations with consolidated assets less than $1 billion.

Nonbank subsidiaries of large complex domestic institutions are covered by the supervisory program. These institutions include nonbank subsidiaries of the parent bank holding company and those of the subsidiary state member banks; the significant branch operations, primarily foreign branches, of state member banks; and subsidiary foreign banks of the holding company. The level of supervisory activity to be conducted for nonbank subsidiaries and foreign branches and subsidiaries of domestic institutions should be based on their individual risk levels relative to the consolidated organization or the state member bank. The risk associated with significant nonbank subsidiaries or branches should be identified as part of the consolidated risk-assessment process. The scope of Edge Act corporation examinations should also be determined through the risk-assessment process. In addition, specialty areas should be included in the planning process in relation to their perceived level of risk to the consolidated organization or to any state member bank subsidiary.

Coordination of Supervisory Activities

Many large complex institutions have interstate operations; therefore, close cooperation with the other federal and state banking agencies is critical. To facilitate coordination between the Federal Reserve and other regulators, District Reserve Banks have been assigned roles and responsibilities that reflect their status as either the responsible Reserve Bank (RRB) with the central point of contact or the local Reserve Bank (LRB).

The RRB is accountable for all aspects of the supervision of a fully consolidated banking organization, which includes the supervision of all the institution's subsidiaries and affiliates (domestic, foreign, and Edge corporations) for which the Federal Reserve has supervisory oversight responsibility. The RRB is generally expected to work with LRBs in conducting examinations and other supervisory activities, particularly where significant banking operations are conducted in a local District. Thus, for state member banks, the LRB has an important role in the supervision of that subsidiary. However, the RRB retains authority and accountabil-

4. Large institutions are defined differently in other regulatory guidance for regulatory reports and examination mandates.

ity for the results of all examinations and reviews that an LRB may perform on its behalf. See SR-05-27/CA-05-11.

Responsible Reserve Bank

In general, the RRB for a banking institution has been the Reserve Bank in the District where the banking operations of the organization are principally conducted. For domestic banking institutions, the RRB typically will be the Reserve Bank District where the head office of the top-tier institution is located and where its overall strategic direction is established and overseen. For foreign banking institutions, the RRB typically will be the Reserve Bank District where the Federal Reserve has the most direct involvement in the day-to-day supervision of the U.S. banking operations of the institution.

When necessary, the Board's Division of Banking Supervision and Regulation (BS&R), in consultation with the Division of Consumer and Community Affairs (C&CA), may designate an RRB when the general principles set forth above could impede the ability of the Federal Reserve to perform its functions under law, do not result in an efficient allocation of supervisory resources, or are otherwise not appropriate.

Duties of RRBs

The RRB develops the consolidated risk assessment and supervisory plan and ensures that the scope and timing of planned activities conducted by participating Districts and agencies pursuant to the plan are appropriate, given the consolidated risk assessment. The RRB designates the central point of contact or lead examiner and ensures that all safety-and-soundness, information technology, trust, consumer compliance, Community Reinvestment Act (CRA), and other specialty examinations, inspections, and visitations are conducted and appropriately coordinated within the System and with other regulators. In addition, the RRB manages all formal communications with the foreign and domestic supervised entity, including the the communication of supervisory assessments, ratings, and remedial actions.[5]

5. See SR-97-24, "Risk-Focused Framework for Supervision of Large Complex Institutions," and SR-96-33, "State/Federal Protocol and Nationwide Supervisory Agreement."

Sharing of RRB Duties

To take advantage of opportunities to enhance supervisory effectiveness or efficiency, an RRB is encouraged to arrange for the LRB to undertake on its behalf certain examinations or other supervisory activities. For example, an LRB may have relationships with local representatives of the institution or local supervisors; leveraging these relationships may facilitate communication and reduce costs. Additionally, LRBs may provide specialty examination resources—in the case of CRA examinations, LRB staff often provide valuable insights into local communities and lending institutions that should be factored into the CRA assessment. When other Reserve Bank Districts conduct examinations and other supervisory activities for the RRB, substantial reliance should be placed on the conclusions and ratings recommended by the participating Reserve Bank(s).

The RRB retains authority and accountability for the results of all examinations and reviews performed on its behalf and, therefore, must work closely with LRB examination teams to ensure that examination scopes and conclusions are consistent with the supervisory approach and message applied across the consolidated organization. If an LRB identifies major issues in the course of directly conducting supervisory activities on behalf of an RRB, those issues should be brought to the attention of the RRB in a timely manner.

If an RRB arranges for an LRB to conduct supervisory activities on its behalf, the LRB is responsible for the costs of performing the activities. If the LRB is unable to fulfill the request from the RRB to perform the specified activities, the RRB should seek System assistance, if needed, by contacting Board staff or using other established procedures for coordinating resources.

In general, LRBs are responsible for the direct supervision of state member banks located in their district. LRBs and host states will not routinely examine branches of state member banks or issue separate ratings and reports of examination. Similar to the relationship between the RRBs and LRBs, home-state supervisors[6]

6. The State/Federal Supervisory Protocol and Agreement established definitions for home and host states. The home-state supervisor is defined as the state that issued the charter. It will act on behalf of itself and all host-state supervisors (states into which the bank branches) and will be the single state contact for a particular institution.

will coordinate the activities of all state banking departments and will be the state's principal source of contact with federal banking agencies and with the bank itself. Also, host states will not unilaterally examine branches of interstate banks. Close coordination among the Reserve Banks and other appropriate regulators for each organization is critical to ensure a consistent, risk-focused approach to supervision.

Central Point of Contact and Supervisory Teams

A central point of contact is critical to fulfilling the objectives of seamless, risk-focused supervision. The RRB should designate a central point of contact for each large complex institution it supervises. Generally, all activities and duties of other areas within the Federal Reserve, as well as those conducted with other supervisors, should be coordinated through this contact. The central point of contact should—

- be knowledgeable, on an ongoing basis, about the institution's financial condition, management structure, strategic plan and direction, and overall operations;
- remain up-to-date on the condition of the assigned institution and be knowledgeable regarding all supervisory activities; monitoring and surveillance information; applications issues; capital-markets activities; meetings with management; and enforcement issues, if applicable;
- ensure that the objective of seamless, risk-focused supervision is achieved for each institution and that the supervisory products described later are prepared in a timely manner;
- ensure appropriate follow-up and tracking of supervisory concerns, corrective actions, or other matters that come to light through ongoing communications or surveillance; and
- participate in the examination process, as needed, to ensure consistency with the institution's supervisory plan and to ensure effective allocation of resources, including coordination of on-site efforts with specialty examination areas and other supervisors, as appropriate, and to facilitate requests for information from the institution, whenever possible.

A dedicated supervisory team composed of individuals with specialized skills based upon the organization's particular business lines and risk profile will be assigned to each institution. This full-time, dedicated cadre will be supplemented by other specialized System staff, as necessary, to participate in examinations and targeted reviews.

In addition to designing and executing the supervisory strategy for an organization, the central point of contact is responsible for managing the supervisory team. The supervisory team's major responsibilities are to maintain a high level of knowledge of the banking organization and to ensure that supervisory strategies and priorities are consistent with the identified risks and institutional profile.

Sharing of Information

To further promote seamless, risk-focused supervision, information related to a specific institution should be provided, as appropriate, to other interested supervisors. The information to be shared includes the products described in the "Process and Products" subsection. However, sharing these products with the institution itself should be carefully evaluated on a case-by-case basis.

Confidentiality Provisions in Agreements that Prevent or Restrict Notification to the Federal Reserve

The Federal Reserve has stated and clarified its expectations regarding confidentiality provisions that are contained in agreements between a banking organization and its counterparties (for example, mutual funds, hedge funds, and other trading counterparties) or other third parties. It is contrary to Federal Reserve's regulations and policy for agreements to contain confidentiality provisions that (1) restrict the banking organization from providing information to Federal Reserve supervisory staff;[6a] (2) require or permit, without the prior approval of the Federal Reserve, the banking organization to disclose to a counterparty that any information will be or was provided to Federal Reserve supervisory

6a. Supervisory staff include individuals that are on and/or off site.

staff; or (3) require or permit, without the prior approval of the Federal Reserve, the banking organization to inform a counterparty of a current or upcoming Federal Reserve examination or any nonpublic Federal Reserve supervisory initiative or action. Banking organizations that have entered, or enter, into agreements containing such confidentiality provisions are subject to legal risk. (See SR-07-19 and SR-97-17.) For information on the restrictions pertaining to the very limited disclosure of confidential supervisory ratings and other nonpublic supervisory information, see SR-05-4, SR-96-26, and SR-88-37. See also section 5020.1.

Functional Approach and Targeted Examinations

Traditionally, the examination process has been driven largely by a legal-entity approach to banking companies. The basis for risk-focused supervision of large complex institutions relies more heavily on a functional, business-line approach to supervising institutions, while effectively integrating the functional approach into the legal-entity assessment.

The functional approach focuses principally on the key business activities (for example, lending, Treasury, retail banking) rather than on reviewing the legal entity and its balance sheet. This approach does not mean that the responsibility for a legal-entity assessment is ignored, nor should the Federal Reserve perform examinations of institutions that other regulators are primarily responsible for supervising.[7] Rather, Federal Reserve examiners should integrate the findings of a functional review into the legal-entity assessment and coordinate closely with the primary regulator to gather sufficient information to form an assessment of the consolidated organization. Nonetheless, in some cases, effective supervision of the consolidated organization may require Federal Reserve examiners to perform process reviews and possibly transaction testing at all levels of the organization.

Functional risk-focused supervision is to be achieved by—

7. For U.S. banks owned by FBOs, it is particularly important to review the U.S. bank on a legal-entity basis and to review the risk exposure to the U.S. bank of its parent foreign bank since U.S. supervisory authorities do not supervise or regulate the parent bank.

- planning and conducting joint examinations with the primary regulator in areas of mutual interest, such as nondeposit investment products, interest-rate risk, liquidity, and mergers and acquisitions;
- leveraging off, or working from, the work performed by the primary regulator and the work performed by the institution's internal and external auditors by reviewing and using their workpapers and conclusions to avoid duplication of effort and to lessen the burden on the institution;
- reviewing reports of examinations and other communications to the institution issued by other supervisors; and
- conducting a series of functional reviews or targeted examinations of business lines, relevant risk areas, or areas of significant supervisory concern during the supervisory cycle. Functional reviews and targeted examinations are increasingly necessary to evaluate the relevant risk exposure of a large, complex institution and the effectiveness of related risk-management systems.

The relevant findings of functional reviews or targeted examinations should be—

- incorporated into the annual summary supervisory report, with follow-up on deficiencies noted in the functional reviews or targeted examinations;
- conveyed to the institution's management during a close-out or exit meeting with the relevant area's line management; and
- communicated in a formal written report to the institution's management or board of directors when significant weaknesses are detected or when the finding results in a downgrade of any rating component.

The functional approach to risk assessments and to planning supervisory activities should include a review of the parent company and its significant nonbank subsidiaries. However, the level of supervisory review should be appropriate to the risk profile of the parent company or its nonbank subsidiary in relation to the consolidated organization. Intercompany transactions should continue to be reviewed as part of the examination procedures performed to ensure that these transactions comply with laws and regulations and do not pose safety-and-soundness concerns.

Process and Products

The risk-focused methodology for the supervision program for large, complex institutions reflects a continuous and dynamic process. The methodology consists of six steps, each of which uses certain written products to facilitate communication and coordination.

Table 1—Steps and Products

Steps	*Products*
1. Understanding the institution	1. Institutional overview
2. Assessing the institution's risk	2. Risk matrix 3. Risk assessment
3. Planning and scheduling supervisory activities	4. Supervisory plan 5. Examination program
4. Defining examination activities	6. Scope memorandum 7. Entry letter
5. Performing examination procedures	8. Functional examination modules
6. Reporting the findings	9. Examination report(s)

The focus of the products should be on fully achieving a risk-focused, seamless, and coordinated supervisory process, not simply on completing the products. The content and format of the products are flexible and should be adapted to correspond to the supervisory practices of the agencies involved and to the structure and complexity of the institution.

Understanding the Institution

The starting point for risk-focused supervision is developing an understanding of the institution. This step is critical to tailoring the supervision program to meet the characteristics of the organization and to adjusting that program on an ongoing basis as circumstances change. Furthermore, understanding the Federal Reserve's

supervisory role in relation to an institution and its affiliates is essential.

Through increased emphasis on planning and monitoring, supervisory activities can focus on the significant risks to the institution and on related supervisory concerns. The technological and market developments within the financial sector and the speed with which an institution's financial condition and risk profile can change make it critical for supervisors to keep abreast of events and changes in risk exposure and strategy. Accordingly, the central point of contact for each large, complex institution should review certain information on an ongoing basis and prepare an institution overview that will communicate his or her understanding of that institution.

Information generated by the Federal Reserve, other supervisory agencies, the institution, and public organizations may assist the central point of contact in forming and maintaining an ongoing understanding of the institution's risk profile and current condition. In addition, the central point of contact should hold periodic discussions with the institution's management to cover, among other topics, credit-market conditions, new products, divestitures, mergers and acquisitions, and the results of any recently completed internal and external audits. When other agencies have supervisory responsibilities for the organization, joint discussions should be considered.

The principal risk-focused supervisory tools and documents, including an institutional overview, risk matrix, and risk assessment for the organization, should be current. Accordingly, the central point of contact should distill and incorporate significant new information into these documents at least quarterly. Factors such as emerging risks; new products; and significant changes in business strategy, management, condition, or ownership may warrant more frequent updates. In general, the more dynamic the organization's operations and risks, the more frequently the central point of contact should update the risk assessment, strategies, and plans.

Preparation of the Institutional Overview

The institutional overview should contain a concise executive summary that demonstrates an understanding of the institution's present condition and its current and prospective risk profiles, as well as highlights key issues and past supervisory findings. General types of information that may be valuable to present in the overview include—

- a brief description of the organizational structure;
- a summary of the organization's business strategies as well as changes in key business lines, growth areas, new products, etc., since the prior review;
- key issues for the organization, either from external or internal factors;
- an overview of management;
- a brief analysis of the consolidated financial condition and trends;
- a description of the future prospects of the organization;
- descriptions of internal and external audit;
- a summary of supervisory activity performed since the last review; and
- considerations for conducting future examinations.

Assessing the Institution's Risks

To focus supervisory activities on the areas of greatest risk to an institution, the central point of contact should perform a risk assessment. The risk assessment highlights both the strengths and vulnerabilities of an institution and provides a foundation for determining the supervisory activities to be conducted. Further, the assessment should apply to the entire spectrum of risks facing an institution (as previously discussed in the subsection "Risk-Management Processes and Internal Controls").

An institution's business activities present various combinations and concentrations of the noted risks depending on the nature and scope of the particular activity. Therefore, when conducting the risk assessment, consideration must be given to the institution's overall risk environment, the reliability of its internal risk management, the adequacy of its information technology systems, and the risks associated with each of its significant business activities.

Assessment of the Overall Risk Environment

The starting point in the risk-assessment process is an evaluation of the institution's risk tolerance

and of management's perception of the organization's strengths and weaknesses. This evaluation should entail discussions with management and review of supporting documents, strategic plans, and policy statements. In general, management is expected to have a clear understanding of both the institution's markets and the general banking environment, as well as how these factors affect the institution.

The institution should have a clearly defined risk-management structure, which may be formal or informal, centralized or decentralized. However, the greater the risk assumed by the institution, the more sophisticated its risk-management system should be. Regardless of the approach, the types and levels of risk an institution is willing to accept should reflect its risk appetite, as determined by the board of directors.

To assess the overall risk environment, the central point of contact should make a preliminary evaluation of the institution's internal risk management, considering the adequacy of its internal audit, loan-review, and compliance functions. External audits also provide important information on the institution's risk profile and condition, which may be used in the risk assessment.

In addition, the central point of contact should review risk assessments developed by the internal audit department for significant lines of business, and compare those results with the supervisory risk assessment. Management's ability to aggregate risks on a global basis should also be evaluated. This preliminary evaluation can be used when developing the scope of examination activities to determine the level of examiner reliance on the institution's internal risk management.

Risk-monitoring activities must be supported by management information systems that provide senior managers and directors with timely and reliable reports on the financial condition, operating performance, and risk exposure of the consolidated organization. These systems must also provide managers engaged in the day-to-day management of the organization's activities with regular and sufficiently detailed reports for their areas of responsibility. Moreover, in most large, complex institutions, management information systems not only provide reporting systems, but also support a broad range of business decisions through sophisticated risk-management and decision-making tools such as credit-scoring and asset/liability models and automated trading systems. Accordingly, the institution's risk assessment must consider the adequacy of its information technology systems.

Preparation of the Risk Matrix

A risk matrix is used to identify significant activities, the type and level of inherent risks in these activities, and the adequacy of risk management over these activities, as well as to determine composite-risk assessments for each of these activities and the overall institution. A risk matrix can be developed for the consolidated organization, for a separate affiliate, or along functional business lines. The matrix is a flexible tool that documents the process followed to assess the overall risk of an institution and is a basis for preparation of the narrative risk assessment.

Activities and their significance can be identified by reviewing information from the institution, the Reserve Bank, or other supervisors. After the significant activities are identified, the type and level of risk inherent in them should be determined. Types of risk may be categorized as previously described or by using categories defined either by the institution or other supervisory agencies. If the institution uses risk categories that differ from those defined by the supervisory agencies, the examiner should determine if all relevant types of risk are appropriately captured. If risks are appropriately captured by the institution, the examiner should use the categories identified by the institution.

For the identified functions or activities, the inherent risk involved in that activity should be described as high, moderate, or low for each type of risk associated with that type of activity. The following definitions apply:

- *High inherent risk* exists when the activity is significant or positions are large in relation to the institution's resources or its peer group, when the number of transactions is substantial, or when the nature of the activity is inherently more complex than normal. Thus, the activity potentially could result in a significant and harmful loss to the organization.
- *Moderate inherent risk* exists when positions are average in relation to the institution's resources or its peer group, when the volume of transactions is average, and when the activity is more typical or traditional. Thus, while the activity potentially could result in a

loss to the organization, the loss could be absorbed by the organization in the normal course of business.
- *Low inherent risk* exists when the volume, size, or nature of the activity is such that even if the internal controls have weaknesses, the risk of loss is remote, or, if a loss were to occur, it would have little negative impact on the institution's overall financial condition.

This risk-assessment is made without considering management processes and controls; those factors are considered when evaluating the adequacy of the institution's risk-management systems.

Assessing Adequacy of Risk Management

When assessing the adequacy of an institution's risk-management systems for identified functions or activities, the focus should be on findings related to the key elements of a sound risk-management system: active board and senior management oversight; adequate policies, procedures, and limits; adequate risk-management, monitoring, and management information systems; and comprehensive internal controls. (These elements are described in the earlier subsection ''Elements of Risk Management.'')

Taking these key elements into account, the contact should assess the relative strength of the risk-management processes and controls for each identified function or activity. Relative strength should be characterized as strong, acceptable, or weak as defined below:

- *Strong risk management* indicates that management effectively identifies and controls all major types of risk posed by the relevant activity or function. The board and management participate in managing risk and ensure that appropriate policies and limits exist, which the board understands, reviews, and approves. Policies and limits are supported by risk-monitoring procedures, reports, and management information systems that provide the necessary information and analysis to make timely and appropriate responses to changing conditions. Internal controls and audit procedures are appropriate to the size and activities of the institution. There are few exceptions to established policies and procedures, and none of these exceptions would likely lead to a significant loss to the organization.
- *Acceptable risk management* indicates that the institution's risk-management systems, although largely effective, may be lacking to some modest degree. It reflects an ability to cope successfully with existing and foreseeable exposure that may arise in carrying out the institution's business plan. While the institution may have some minor risk-management weaknesses, these problems have been recognized and are being addressed. Overall, board and senior management oversight, policies and limits, risk-monitoring procedures, reports, and management information systems are considered effective in maintaining a safe and sound institution. Risks are generally being controlled in a manner that does not require more than normal supervisory attention.
- *Weak risk management* indicates risk-management systems that are lacking in important ways and, therefore, are a cause for more than normal supervisory attention. The internal control system may be lacking in important respects, particularly as indicated by continued control exceptions or by the failure to adhere to written policies and procedures. The deficiencies associated in these systems could have adverse effects on the safety and soundness of the institution or could lead to a material misstatement of its financial statements if corrective actions are not taken.

The composite risk for each significant activity is determined by balancing the overall level of inherent risk of the activity with the overall strength of risk-management systems for that activity. For example, commercial real estate loans usually will be determined to be inherently high risk. However, the probability and the magnitude of possible loss may be reduced by having very conservative underwriting standards, effective credit administration, strong internal loan review, and a good early warning system. Consequently, after accounting for these mitigating factors, the overall risk profile and level of supervisory concern associated with commercial real estate loans may be moderate.

To facilitate consistency in the preparation of the risk matrix, general definitions of the composite level of risk for significant activities are provided as follows:

- A *high composite risk* generally would be assigned to an activity in which the risk-

management system does not significantly mitigate the high inherent risk of the activity. Thus, the activity could potentially result in a financial loss that would have a significant negative impact on the organization's overall condition, in some cases, even when the systems are considered strong. For an activity with moderate inherent risk, a risk-management system that has significant weaknesses could result in a high composite risk assessment because management appears to have an insufficient understanding of the risk and uncertain capacity to anticipate and respond to changing conditions.

- A *moderate composite risk* generally would be assigned to an activity with moderate inherent risk, which the risk-management systems appropriately mitigate. For an activity with low inherent risk, significant weaknesses in the risk-management system may result in a moderate composite risk assessment. On the other hand, a strong risk-management system may reduce the risks of an inherently high-risk activity so that any potential financial loss from the activity would have only a moderate negative impact on the financial condition of the organization.
- A *low composite risk* generally would be assigned to an activity that has low inherent risks. An activity with moderate inherent risk may be assessed a low composite risk when internal controls and risk-management systems are strong, and when they effectively mitigate much of the risk.

Once the composite risk assessment of each identified significant activity or function is completed, an overall composite risk assessment should be made for off-site analytical and planning purposes. This assessment is the final step in the development of the risk matrix, and the evaluation of the overall composite risk is incorporated into the written risk assessment.

Preparation of the Risk Assessment

A written risk assessment is used as an internal supervisory planning tool and to facilitate communication with other supervisors. The goal is to develop a document that presents a comprehensive, risk-focused view of the institution, delineating the areas of supervisory concern and serving as a platform for developing the supervisory plan.

The format and content of the written risk assessment are flexible and should be tailored to the individual institution. The risk assessment reflects the dynamics of the institution; therefore, it should consider the institution's evolving business strategies and be amended as significant changes in the risk profile occur. Input from other affected supervisors and specialty units should be included to ensure that all the institution's significant risks are identified. The risk assessment should—

- include an overall risk assessment of the organization;
- describe the types of risk (credit, market, liquidity, reputational, operational, legal) and their level (high, moderate, low) and direction (increasing, stable, decreasing);
- identify all major functions, business lines, activities, products, and legal entities from which significant risks emanate, as well as the key issues that could affect the risk profile;
- consider the relationship between the likelihood of an adverse event and its potential impact on an institution; and
- describe the institution's risk-management systems. Reviews and risk assessments performed by internal and external auditors should be discussed, as should the institution's ability to take on and manage risk prospectively.

The central point of contact should attempt to identify the cause of unfavorable trends, not just report the symptoms. The risk assessment should reflect a thorough analysis that leads to conclusions about the institution's risk profile, rather than just reiterating the facts.

Planning and Scheduling Supervisory Activities

The supervisory plan forms a bridge between the institution's risk assessment, which identifies significant risks and supervisory concerns, and the supervisory activities to be conducted. In developing the supervisory plan and examination schedule, the central point of contact should minimize disruption to the institution and, whenever possible, avoid duplicative examination efforts and requesting similar information from the other supervisors.

The institution's organizational structure and complexity are significant considerations when planning the specific supervisory activities to be conducted. Additionally, interstate banking and branching activities have implications for planning on-site and off-site review. The scope and location of on-site work for interstate banking operations will depend upon the significance and risk profile of local operations, the location of the supervised entity's major functions, and the degree of its centralization. The bulk of safety-and-soundness examinations for branches of an interstate bank would likely be conducted at the head office or regional offices, supplemented by periodic reviews of branch operations and internal controls. The supervisory plan should reflect the need to coordinate these reviews of branch operations with other supervisors.

Preparation of the Supervisory Plan

A comprehensive supervisory plan should be developed annually, and reviewed and revised at least quarterly to reflect any significant new information or emerging banking trends or risks. The supervisory plan and any revisions should be periodically discussed with representatives of the principal regulators of major affiliates to reconfirm their agreement on the overall plan for coordinating its implementation, when warranted.

The plan should demonstrate that both the supervisory concerns identified through the risk-assessment process and the deficiencies noted in the previous examination are being or will be addressed. To the extent that the institution's risk-management systems are adequate, the level of supervisory activity may be adjusted. The plan should generally address all supervisory activities to be conducted, the scope of those activities (full or targeted), the objectives of those activities (for example, review of specific business lines, products, support functions, legal entities), and specific concerns regarding those activities, if any. Consideration should be given to—

- prioritizing supervisory resources on areas of higher risk;
- pooling examiner resources to reduce the regulatory burden on institutions as well as examination redundancies;
- maximizing the use of examiners who are located where the activity is being conducted;
- coordinating examinations of different disciplines;
- determining compliance with, or the potential for, supervisory action;
- balancing mandated requirements with the objectives of the plan;
- providing general logistical information (for exammple, a timetable of supervisory activities, the participants, and expected resource requirements); and
- assessing the extent to which internal and external audit, internal loan review, compliance, and other risk-management systems will be tested and relied upon.

Generally, the planning horizon to be covered is 18 months for domestic institutions.[8] The overall supervisory objectives and basic framework need to be outlined by midyear to facilitate preliminary discussions with other supervisors and to coincide with planning for the Federal Reserve's annual scheduling conferences. The plan should be finalized by the end of the year, for execution in the following year.

Preparation of the Examination Program

The examination program should provide a comprehensive schedule of examination activities for the entire organization and aid in the coordination and communication of responsibilities for supervisory activities. An examination program provides a comprehensive listing of all examination activities to be conducted at an institution for the given planning horizon. To prepare a complete examination program and reflect the institution's current conditions and activities, and the activities of other supervisors, the central point of contact needs to be the focal point for communications on a particular institution. The role includes any communications with the Federal Reserve, the institution's management, and other supervisors. The examination program generally incorporates the following logistical elements:

- a schedule of activities, period, and resource estimates for planned projects

8. The examination plans and assessments of condition of U.S. operations that are used for FBO supervision use a 12-month period.

- an identification of the agencies conducting and participating in the supervisory activity (when there are joint supervisors, indicate the lead agency and the agency responsible for a particular activity) and resources committed by all participants to the area(s) under review
- the planned product for communicating findings (indicate whether it will be a formal report or supervisory memorandum)
- the need for special examiner skills and the extent of participation of individuals from specialty functions

Defining Examination Activities

Scope Memorandum

The scope memorandum is an integral product in the risk-focused methodology because it identifies the key objectives of the on-site examination. The focus of on-site examination activities, identified in the scope memorandum, follow a top-down approach that includes a review of the organization's internal risk-management systems and an appropriate level of transaction testing. The risk-focused methodology is flexible regarding the amount of on-site transaction testing used. Although the focus of the examination is on the institution's processes, an appropriate level of transaction testing and asset review will be necessary to verify the integrity of internal systems.

After the areas to be reviewed have been identified in the supervisory plan, a scope memorandum should be prepared that documents specific objectives for the projected examinations. This document is of key importance, as the scope of the examination will likely vary from year to year. Thus, it is necessary to identify the specific areas chosen for review and the extent of those reviews. The scope memorandum will help ensure that the supervisory plan for the institution is executed and will communicate the specific examination objectives to the examination staff.

The scope memorandum should be tailored to the size, complexity, and current rating of the institution subject to review. For large but less-complex institutions, the scope memorandum may be combined with the supervisory plan or the risk assessment. The scope memorandum should define the objectives of the examination, and generally should include—

- a statement of the objectives;
- an overview of the activities and risks to be evaluated;
- the level of reliance on internal risk-management systems and internal or external audit findings;
- a description of the procedures that are to be performed, indicating any sampling process to be used and the level of transaction testing, when appropriate;
- identification of the procedures that are expected to be performed off-site; and
- a description of how the findings of targeted reviews, if any, will be used on the current examination.

Entry Letter

The entry letter should be tailored to fit the specific character and profile of the institution to be examined and the scope of the activities to be performed. Thus, effective use of entry letters depends on the planning and scoping of a risk-focused examination. To eliminate duplication and minimize the regulatory burden on an institution, entry letters should not request information that is regularly provided to designated central points of contact or that is available within each Federal Reserve Bank. When needed for examinations of larger or more complex organizations, the entry letter should be supplemented by requests for information on specialty activities. The specific items selected for inclusion in the entry letter should meet the following guidelines:

- reflect risk-focused supervision objectives and the examination scope
- facilitate efficiency in the examination process and lessen the burden on financial institutions
- limit, to the extent possible, requests for special management reports
- eliminate items used for audit-type procedures (for example, verifications)
- distinguish between information to be mailed to the examiner-in-charge for off-site examination procedures and information to be held at the institution for on-site procedures
- allow management sufficient lead time to prepare the requested information

Examination Procedures

Examination procedures should be tailored to the characteristics of each institution, keeping in mind size, complexity, and risk profile. They should focus on developing appropriate documentation to adequately assess management's ability to identify, measure, monitor, and control risks. Procedures should be completed to the degree necessary to determine whether the institution's management understands and adequately controls the levels and types of risks that are assumed. For transaction testing, the volume of loans to be tested should be adjusted according to management's ability to accurately identify problems and potential problem credits and to measure, monitor, and control the institution's exposure to overall credit risk. Likewise, the level of transaction testing for compliance with laws and regulations should take into account the effectiveness of management systems to monitor, evaluate, and ensure compliance with applicable laws and regulations.

During the supervisory cycle, the 10 functional areas listed below will be evaluated in most full-scope examinations. To evaluate these functional areas, procedures need to be tailored to fit the risk assessment that was prepared for the institution and the scope memorandum that was prepared for the examination. These functional areas represent the primary business activities and functions of large complex institutions as well as common sources of significant risk to them. Additionally, other areas of significant sources of risk to an institution or areas that are central to the examination assignment will need to be evaluated. The functional areas include the following:

- loan portfolio analysis
- Treasury activities
- trading and capital-markets activities
- internal controls and audit
- supervisory ratings
- information systems
- fiduciary activities
- private banking
- retail banking activities
- payments system risk

Reporting the Findings

At least annually, a comprehensive summary supervisory report should be prepared that supports the organization's assigned ratings and encompasses the results of the entire supervisory cycle. This report should (1) convey the Federal Reserve's view of the condition of the organization and its key risk-management processes, (2) communicate the composite supervisory ratings, (3) discuss each of the major business risks, (4) summarize the supervisory activities conducted during the supervisory cycle and the resulting findings, and (5) assess the effectiveness of any corrective actions taken by the organization. This report will satisfy supervisory and legal requirements for a full-scope examination. Reserve Bank management, as well as Board officials, when warranted, will meet with the organization's board of directors to present and discuss the contents of the report and the Federal Reserve's assessment of the condition of the organization. (See SR-99-15.)

Minimum Timing Standards for Examination Report Completion

Examination reports issued by the Federal Reserve must be completed and filed within a maximum of 60 calendar days, commencing with the day following the examiner's exit meeting. This standard applies to reports for all banks, regardless of the complexity of the organization. Additionally, for instructions with a CAMELS composite rating of 3, 4, or 5, Reserve Banks are encouraged to adopt an internal target of 45 calendar days for processing and filing reports. In cases where reports are issued jointly with other agencies, this standard may be extended at the discretion of senior management at the Reserve Bank. (See SR-93-4.)

Internal Control and Audit Function, Oversight, and Outsourcing

Effective date October 2008

Section 1010.1

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.

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 growing in importance. 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 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.

1. For state member banks, see appendix D-1 to 12 CFR 208.

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.)

In May 2003, the Federal Reserve, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision announced that they did not expect to take actions to apply the corporate-governance and other requirements of the Sarbanes-Oxley Act generally to nonpublic banking organizations that are not otherwise subject to them.[2] (See SR-03-08.) 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)[3] 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,[3a] an accountant or firm from performing audit and attesta-

2. Some aspects of the auditor-independence rules established by the Sarbanes-Oxley Act apply to all federally insured depository institutions with $500 million or more in total assets. See part 363 of the FDIC's regulations.

3. 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. The Board approved its rules on August 6, 2003 (press release of August 8, 2003). The rules became effective October 1, 2003.

3a. 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.

tion services for insured depository institutions with assets of $500 million or more.[3b] Immediate suspensions are permitted in limited circumstances. 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

3b. 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.

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 circumstances 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 but Less Than $1 Billion in Total Assets

The regulations require these institutions to file an annual report with the FDIC 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 over financial reporting;
    - complying with the laws and regulations relating to safety and soundness that are designated by the FDIC and the appropriate federal banking agency; and
  - — An assessment by management of the institution's compliance with the designated laws and regulations during the fiscal year.

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 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 an annual report that must include the following:

- Audited comparative annual financial statements;
- The independent public accountant's report on the audited financial statements;
- A management report that contains:
  - — A statement of management's responsibilities for:
    - Preparing the annual financial statements;
    - Establishing and maintaining an adequate internal control structure over financial reporting;
    - Complying with the laws and regulations relating to safety and soundness that are designated by the FDIC and the appropriate federal banking agency; and
  - — 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 institution's compliance with safety and soundness laws and regulations during the year (12 USC 1831n(b)(2)(B)(ii)); 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)). 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)),

Each institution must file with the FDIC two copies of the annual report within 90 days after the end of its fiscal year. Notwithstanding the 90-day filing period, each institution must file a copy of each audit and attestation report issued by its independent accountant within 15 days of their receipt.

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.

For insured institutions having total assets of more than $3 billion, the audit committee must (1) have members with banking or related financial management expertise, (2) have access to outside legal counsel, and (3) not include any large customers of the institution. The audit committee also may be required to satisfy other audit committee membership criteria (12 USC

831m (g)(1)(c)) and section 363.5(b) (12 CFR 363.5(b)).

Any covered institution with a composite CAMELS rating of 1 or 2 may file the two above-mentioned reports through its parent holding company on a consolidated basis. The Guidelines and Interpretations (appendix A to Part 363) provide that one of the duties of a covered institution's audit committee should include oversight of the internal audit function and its operations. (See SR-96-4.)

INTERAGENCY POLICY STATEMENT ON THE INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING

The Federal Reserve and other federal banking agencies[3c] (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.

Internal Audit Function (Part I)

Board and Senior Management Responsibilities

The board of directors and senior management

3c. The Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

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.[4]

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,[5] using objective criteria it has established, should oversee the internal audit function and evaluate its performance.[6] 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 arrangement 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: Relation-*

4. 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.)

5. 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).

6. For example, the performance criteria could include the timeliness of each completed audit, a comparison of overall performance to plan, and other measures.

ship 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 reorganiza-

tions. 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 inde-

pendence, 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.[7]

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.[8] 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.

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

7. 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).

8. When the board of directors fulfills the audit committee responsibilities, the procedures should provide for the submission of employee concerns to an outside director.

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.[9] Contracts between the

9. The engagement-letter provisions described are comparable to those outlined by the American Institute of Certified Public Accountants (AICPA) for financial statement audits.

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;[10]
- 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 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

(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.

10. 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.

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.[11] 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.[12] 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 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 accoun-

11. 15 USC 78*l* and 78o(d).

12. 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.

tant, 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.[13] 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."[14]

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.[15]

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[16] to have its financial statements audited by an independent public accountant.[17] 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.

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.[18] In this regard, the audit

13. 12 CFR 363.3(a). (See FDIC Financial Institutions Letter FIL-17-2003 (Corporate Governance, Audits, and Reporting Requirements), attachment II, March 5, 2003.)

14. Appendix A to part 363, Guidelines and Interpretations, paragraph 14, Independence.

15. 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.

16. 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.

17. See, for example, the 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Institutions.

18. 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

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.[19]

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 independence 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;

performance of these services on the auditor's independence.

19. 15 USC 78j-1.

- 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 examiner 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.*

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 organiza-

tions 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 determine 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 concern-

ing 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.[20] 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 (insti-

20. See 64 *Fed. Reg.* 52319 (September 28, 1999).

tution) 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),[21] the institution should maintain effective systems and internal control[22] to produce reliable and accurate financial reports.

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[23] 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'[24] 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.

21. 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.

22. This policy statement provides guidance consistent with the guidance established in the Interagency Policy Statement on the Internal Audit Function and Its Outsourcing.

23. 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.

24. Terms are defined at the end of the policy statement.

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.[25] However, if this is impracticable, the board should organize the 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

25. 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.

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.[26] This type of engagement is performed under generally accepted standards for attestation engagements (GASAE).[27]

26. 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.

27. 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.

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 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.[28] 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

28. 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.

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.

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.[29] 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

29. 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.

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 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[30] 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.[31] 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

30. 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.

31. 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.

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 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)[32] 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.[33] The advisory informs financial institutions'[34] 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

32. 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).

33. The advisory is effective for audit engagement letters issued on or after February 9, 2006.

34. As used in this advisory, the term *financial institutions* includes banks, bank holding companies, savings associations, savings and loan holding companies, and credit unions.

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 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,[34a] "[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.[35] 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, agree-

34a. See 64 *Fed. Reg.* 52319 (September 28, 1999).

35. 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.

ments 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 to have annual independent audits.[36] Furthermore, financial institutions that are public companies[37] 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.[38] 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.[39] 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 on

36. For banks, see section 36 of the FDI Act (12 USC 1831m) and part 363 of the FDIC's regulations (12 CFR 363).

37. Public companies are companies subject to the reporting requirements of the Securities Exchange Act of 1934.

38. 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.''*

39. 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.

auditors' 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.

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 audi-

tor'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 organi-

zation 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.

1. To determine whether internal and external audit functions exist.
2. To determine with reasonable assurance that the bank has an adequate internal audit function that ensures efficient and effective operations, including the safeguarding of assets, reliable financial reporting, and compliance with applicable laws and regulations.
3. To ascertain, through the examination process, that the bank's internal audit function monitors, reviews, and ensures the continued existence and maintenance of sound and adequate internal controls over the bank's management process—the control environment, risk assessment, control activities, information and communication, and monitoring activities.
4. To review and evaluate internal audit outsourcing arrangements and the actions of the outsourcing vendor under the standards established by the Interagency Policy Statement on the Internal Audit Function and Its Outsourcing.
5. To evaluate the independence and competence of those who provide the internal and external audit functions.
6. To consider the policies, processes, and personnel surrounding the bank's external auditing program and to determine if—
   a. any engagement letter or other agreement related to external audit activities for the bank (1) provides any assurances of indemnification to the bank's external auditors that relieves them of liability for their own negligent acts (including any losses, claims, damages, or other liabilities) or (2) raises any other safety-and soundness-concerns; and
   b. the external auditors have maintained appropriate independence in their relationships with the bank, in accordance with relevant professional standards.
7. To determine the adequacy of the procedures performed by the internal and external auditors.
8. To determine, based on the criteria above, if the work performed by internal and external auditors is reliable.

This examination program must be used in conjunction with the audit function and audit outsourcing questionnaire section to review the bank's internal and external audits and the audit procedures they encompass. The audit guidelines are general and all sections or questions may not be applicable to every bank.

Before reviewing any specific audit procedures, the examiner should first determine the independence and competence of the auditors. If the examiner believes the auditors to be both competent and independent, he or she should then determine the acceptability of their work. Based on the answers to the audit function questions and on the auditor's work, the examiner must then determine the scope of the examination. The program and related supporting documentation should be completed in an organized manner and should be retained as part of the examination workpapers.

Upon completion of the program, the examiner should be able to formulate a conclusion on the adequacy of audit coverage. Conclusions about any weaknesses in the internal or external audit work performed for the bank should be summarized and included in the report of examination. Significant recommendations should be discussed with the audit committee and senior bank management. If recommendations are made orally, a memorandum of the discussion should be prepared and included in the workpapers.

INTERNAL AUDITORS

1. *Organizational structure of the audit department.* Review the bylaws and the organization chart of the bank and the minutes of the board's audit or examining committee to determine how effectively the board of directors is discharging its responsibility.
2. *Independence of the audit function.* Interview the auditor and observe the operation of the audit department to determine its functional responsibilities.
3. *Auditors' qualifications.* Review biographical data and interview the auditor to determine his or her ability to manage the auditor's responsibility in the bank.
4. *Audit staff qualifications.* Review the biographical data and interview the management staff of the audit department to determine their qualifications for their delegated responsibilities.
5. *Content and use of the audit frequency and scope schedule.* Review the organization charts and the bank's chart of accounts to determine the adequacy of the audit program.
6. *Audit department participation in systems design projects.* Determine, through interviews with the internal auditor and appropriate staff members and through the documentation review, the department's role in automated and/or manual systems design.
7. *Audit manual.* Review the audit manuals and associated internal control questionnaires to determine the adequacy of the prescribed procedures for the accomplishing the audit objectives.
8. *Maintenance of audit records.* Review a sample of the audit reports and associated workpapers to determine compliance with prescribed procedures and proper documentation.
9. *Audit department's formal reporting procedures.* Review all auditor's reports to the board of directors (audit or examining committee) and a representative sample of the departmental or functional reports, consider their distribution and follow-up procedures, and determine how effectively the audit department responsibility is discharged.
10. *Use and effectiveness of audit computer programs.* Interview the auditor and/or the appropriate staff members regarding the use of the computer and access to the files for audit purposes.

INTERNAL AUDIT FUNCTION ADEQUACY

1. Adjust the scope of the examination if the bank's internal audit function does not sufficiently meet the bank's internal audit needs (whether or not the audit function is outsourced), does not satisfy the Interagency Guidelines Establishing Standards for Safety and Soundness, or is otherwise inadequate.
2. Discuss supervisory concerns and outstand-

ing internal-external audit report comments 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 comments and concerns, bring these matters to the attention of senior management and the board of directors or the audit committee.

3. If material weaknesses in the internal audit function or the internal control system exist, discuss them with appropriate Federal Reserve Bank supervisory staff to determine the appropriate actions (including formal and informal enforcement actions) that should be taken to ensure that the bank corrects the deficiencies.
4. Incorporate conclusions about the bank's internal audit function into the bank's management and composite supervisory ratings.
5. Include in the report of examination comments concerning the adequacy of the internal audit function, significant issues or concerns, and recommended corrective actions.

INDEPENDENCE OF THE OUTSOURCING VENDOR

1. If the initial review of an internal audit outsourcing arrangement, including the actions of the outsourcing vendor, raises questions about the bank's and its vendor's adherence to the independence standards discussed in parts I and II (and also in part III, if the vendor provides both external and internal audit services to the bank) of the Interagency Policy Statement on the Internal Audit Function and Its Outsourcing—
   a. ask the bank and the outsourcing vendor how the audit committee determined that the vendor was independent;
   b. if the vendor is an accounting firm, ask the audit committee how it assessed that the arrangement has not compromised applicable SEC, PCAOB, AICPA, or other regulatory standards concerning auditor independence;
   c. if the answers to the above supervisory concerns are not adequately addressed, discuss the matter with appropriate Reserve Bank supervisory staff; and
   d. if the Reserve Bank supervisory staff concurs that the independence of the external auditor or other vendor appears to be compromised, discuss the examination findings and the supervisory actions that may be taken with the bank's senior management, board of directors (or audit committee), and the external auditor or other vendor.

EXTERNAL AUDITORS

1. If the bank has engaged any external audit firms to conduct audits of its financial statements (including their certification), audits of internal control over financial reporting, attestations on management's assessment of internal control, appraisals of the bank's audit function, any internal audit or audit function or operational review, review any pending or past engagement letters and agreements. Determine if the audit engagement letters or other agreements include unsafe and unsound provisions that—
   a. indemnify the external auditor against all claims made by third parties;
   b. hold harmless, release, or indemnify the external auditor from liability for claims or potential claims that the bank may assert (other than claims for punitive damages), thus providing relief from liability for the auditors' own negligent acts, including any losses, claims, damages, or other liabilities; or
   c. limit the remedies available to the bank (other than punitive damages).
2. Find out whether the bank's board of directors, audit committee, and senior management closely review all of the provisions of audit engagement letters or other agreements for providing external auditing services for the bank before agreeing to sign them, thus indicating the bank's approval and financial commitment.
3. Verify that the bank has documented its business rationale qfor any engagement letter or other agreement provisions with external audit firms that limit or impair the bank's legal rights.
4. With the cooperation of the audit committee, review and determine the adequacy of the bank's external auditors' reports, letters, or correspondence, including their supporting workpapers, for the audit work performed since the previous examination.

REGULATORY EXAMINATIONS

1. Review any functional regulatory examination or supervisory examination report for work performed since the previous state member bank examination. Interview any involved auditors to determine their responsibilities and extent of involvement with the work in this area.

Review the documentation as instructed in the examination procedures section to answer the following audit function and audit outsourcing questions. Where appropriate, supporting documentation and pertinent information should be retained or noted under comments.

ORGANIZATIONAL STRUCTURE AND INTERNAL CONTROL ENVIRONMENT OF THE AUDIT DEPARTMENT

1. Has the board of directors delegated responsibility for the audit function? If so, to whom?
2. Has the board of directors established an audit committee? Is it composed solely of outside directors?
3. Are the members of the audit committee qualified for their particular responsibilities?
4. Does the audit committee promote the internal audit manager's impartiality and independence by having him or her directly report audit findings to it? How often does the audit committee meet with and review reports issued by the auditor?
5. Are the audit committee meetings with the auditor closed to bank personnel?
6. Do the minutes of the audit committee indicate an appropriate interest in the activities and findings?
7. Does the auditor report to the board of directors, the audit committee, or an executive officer who is sufficiently high in the bank's hierarchy? If so, which one? If not, to whom does the auditor report?
8. Are the internal audit function's control risk assessment, audit plans, and audit programs appropriate for the bank's activities?
9. Are internal audit activities consistent with the long-range goals and strategic direction of the bank, and are they responsive to its internal control needs?
10. Do 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?
11. Does the audit function provide high-quality advice and counsel to management and the board of directors on current developments in risk management, internal control, and regulatory compliance?

INDEPENDENCE AND MANAGEMENT OF THE AUDIT FUNCTION

1. Is the audit department functionally segregated from operations in the organizational structure?
2. Does the audit committee review or approve the budget and salary of the auditor? If not, who does?
3. Are the reporting procedures of the auditor independent of the influence of any operating personnel?
4. Is the internal audit function adequately managed to ensure that audit plans are accomplished and the audit results are promptly communicated to the audit committee, senior management, and the board of directors?
5. Has the audit staff been relieved of responsibility for conducting continuous audits?
6. Has the audit department been relieved of responsibility for maintaining duplicate records?
7. Do the responsibilities of the audit staff exclude any duties to be performed in lieu of operating personnel, such as preparation or approval of general ledger entries, official checks, daily reconcilements, dual control, etc.?

AUDITOR'S QUALIFICATIONS

1. Are the auditor's academic credentials comparable to other bank officers who have major responsibilities within the organization?
2. Is the auditor certified (or in the process of becoming certified) as a chartered bank auditor, certified internal auditor, or certified public accountant? If yes, which one (or ones)?
3. Is the auditor's experience in both auditing and banking comparable both in quality and

in duration to that required of the officers assigned major responsibilities?
4. Does the auditor communicate and relate well with all levels of personnel?
5. Does the auditor demonstrate a commitment to continuing education and a current knowledge of the latest developments in banking and auditing technology?
6. Is the auditor dedicated to the standards and ethics of his or her profession (such as those published by the Bank Administration Institute, the Institute of Internal Auditors, and the American Institute of Certified Public Accountants)?

AUDIT STAFF QUALIFICATIONS

1. Is the audit staff sufficient in number to perform its tasks adequately?
2. Is the staff adequately experienced in auditing and banking?
3. Are members of the staff experienced in specialized areas, such as EDP, foreign-exchange trading, trust, and subsidiary activities of the bank?
4. Is there a formal audit training program in effect?
5. Is the number of unfilled vacancies on the audit staff considered reasonable?
6. Is the turnover of audit personnel acceptable?
7. Does management have plans to improve its audit capability, if needed?

CONTENT AND USE OF THE AUDIT FREQUENCY AND SCOPE SCHEDULE

1. Is the audit program formalized and therefore on record as a commitment that can be analyzed and reviewed?
2. Are all important bank functions and services identified as subjects of the audits?
3. Does the audit program include procedures necessary to ensure compliance with the Federal Election Campaign Act and the Foreign Corrupt Practices Act?
4. Does the internal audit department have access to all reports, records, and minutes?
5. Are internal audit activities adjusted for significant changes in the bank's environment, structure, activities, risk exposures, or systems?
6. Does the frequency and scope schedule require approval by the audit committee, the board of directors, regulatory authorities, or others? If so, by whom, and has such approval been obtained?
7. Does the frequency and scope schedule comply with state statutory requirements, if any, for internal audits, including minimum audit standards?
8. Does the auditor periodically report his or her progress in completing the frequency and scope schedule to the board's audit committee?
   a. If not to the board's audit committee, to whom?
   b. Does the committee approve significant deviations, if any, in the original program?
9. Does the auditor prepare a time budget? Are budgeted versus actual time analyses used as a guide in forward planning?
10. Does the depth of coverage appear to be sufficient?
11. Are different entry dates and time periods between reviews scheduled so as to frustrate reliable anticipation of entry dates by auditees?
12. Is the bank's possession of all assets owned or managed in fiduciary capacities subjected to verification?
13. Are controls on opening and closing general ledger and subsidiary accounts adequate and is the auditor formally advised of any changes?
14. If the bank has automated systems, does the program call for the application of independently prepared computer programs that employ the computer as an audit tool?
15. Will the audit staff examine the documentation of all bank systems and produce their own documentation?
16. Are all service-related activities not specifically manifested in general ledger accounts subject to adequate periodic review (for example, supervisory regulations, security, vacation policy, purchases, traveler's checks, and safekeeping)?
17. Will appraisals of administrative control be made for each function, yielding audit comments and suggestions for improvements of operational efficiency?

AUDIT DEPARTMENT PARTICIPATION IN SYSTEMS DESIGN PROJECTS

1. Is there a formal or informal procedure for notifying the auditor of contemplated new systems or systems modifications in the early planning stages?
2. Is the auditor a member of an executive systems planning or steering committee? If not, does the auditor have access to and review the minutes of such committees?
3. Does an audit representative review the activities of systems design teams for audit and internal control requirements? Is the specialized training and experience of the audit staff sufficient to support effective reviews?
4. Does the audit department avoid overparticipation in systems design, modification, and conversion?
5. Is the auditor's "sign-off" on new or modified systems restricted to control and audit trail features?

AUDIT MANUAL

1. Has responsibility for the establishment and maintenance of the audit manual been clearly assigned?
2. Does the audit manual require approval by the board of directors, the audit committee, or others? If so, has such approval been obtained?
3. Is the content of the audit manual independent from adverse influence by other interests, such as operating management or independent CPAs?
4. Is the audit manual current, and are procedures for keeping the manual current adequate?
5. Does the audit manual contain the scope and objective of each audit?
6. Does the manual provide for valid deviations from audit procedures to be officially approved by audit management?
7. Do audit procedures provide for the follow-up of exceptions noted in previous audits?
8. Does the manual prescribe that each audit procedure be cross-referenced to the appropriate audit workpapers?
9. Must an auditor initial each program step as testimony of his or her performance?
10. Does the manual prescribe that full control be established at the time of entry over the records selected for audit?
11. Is proof of subsidiary to control records required?
12. Are subsidiary direct verification programs covering all forms of customer deposit, loan, safekeeping, collateral, collection, and trust accounts included?
13. Are flow charts called for as evidence of thorough analytical auditing?
14. Do the procedures employ scientific sampling techniques that have acceptable reliability and precision?
15. Does the audit manual provide for the resolution of exceptions and deficiencies?
16. Does the audit manual contain provisions for report format and content and an expression of the opinion of the auditor regarding the adequacy, effectiveness, and efficiency of internal controls?
17. For each audit, do audit procedures provide for a documented method of assuring audit management that a proper study and evaluation of existing internal controls has been made, such as an internal control questionnaire or memorandum?
18. Does the audit manual contain a provision for a review and update of the procedures for each audit, where required, upon the audit's completion?
19. Does the audit manual provide for the maintenance of a permanent file for audits conducted?
20. Does the audit manual contain provisions for the formal, standardized preparation and maintenance of workpapers?
21. Are applicable statutory and regulatory requirements included in the audit procedures?

MAINTENANCE OF AUDIT RECORDS

1. Are workpapers arranged and maintained for filing and reference in—
   a. the current file?
   b. the permanent file?
2. Is a reasonable record-retention schedule and departmental index maintained for audit records?
3. Are audit procedures being complied with during each audit?

4. Do the workpapers contain evidence that all significant deviations from standard audit procedures are documented and have received the approval of audit management?
5. Are procedures for preparing and maintaining workpapers being adhered to?
6. Do workpapers adequately document the internal audit work performed and support the audit reports?
7. Do workpapers contain a copy of the audit report, an adequate index, an internal control questionnaire, audit procedures, and other appropriate material?
8. Are workpapers numbered, indexed, and cross-referenced to audit procedures and the workpapers index?
9. Is each workpaper dated and initialed by the preparer?
   a. Are sources of data clearly shown?
   b. Are tick marks explained?
10. From the workpapers, can it be determined how various sample sizes were determined (by judgment or statistical sampling), including the range and confidence level?
11. Do workpapers contain evidence that supervisory personnel of the audit department have reviewed the workpapers and resultant findings?
12. Are all significant or unresolved exceptions noted in workpapers required to be included in the report?
13. Are applicable statutory and regulatory requirements being complied with?

AUDIT DEPARTMENT'S FORMAL REPORTING PROCEDURES

1. Does the auditor submit formal reports? If so, to whom?
2. Do the reports convey to the reader the auditor's general observation of the condition of the operation of the department or function?
   a. Do they adequately reflect the scope of the audit?
   b. Do they contain an opinion of the auditor regarding the adequacy, effectiveness, and efficiency of internal controls?
   c. Do they call for a prompt response, where appropriate?
3. With regard to audit exceptions and recommendations, is the method of resolving differences of opinion between audit and operating management effective?
4. Does the auditor maintain a formal record of all audit reports that contain unresolved recommendations and exceptions?
5. Does the bank promply respond to significant identified internal control weaknesses? Are exceptions and recommendations generally resolved within 90 days?
6. Are audit reports submitted promptly?
7. Are responses received promptly?

USE AND EFFECTIVENESS OF AUDIT COMPUTER PROGRAMS

1. What audit computer programs are used and what are their purposes?
2. Is there a member of the audit staff qualified to write and appraise the quality of audit computer programs?
3. Is the auditor satisfied that he or she has sufficient ''free access'' to the computer files?
4. Are audit programs run on request?
5. Do direct verification programs allow the auditor flexibility in selecting the criteria to be used in determining the sample?
6. Have procedures been established for the development and maintenance of documentation for audit computer programs? Are they adhered to?
7. Are changes to audit programs controlled?

INTERNAL AUDIT OUTSOURCING ARRANGEMENTS

1. If the bank outsources its internal audit function, does it have a written contract or an engagement letter with the vendor?
2. Does the written contract or engagement letter include provisions that—
   a. define the expectations and responsibilities under the contract for both parties?
   b. set the scope and frequency of, and the fees to be paid for, the work to be performed by the vendor?
   c. 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?
   d. establish the process for changing the

terms of the service contract, especially for expansion of audit work if significant issues are found, and contain stipulations for default and termination of the contract?
   e. 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?
   f. specify the locations of internal audit reports and the related workpapers?
   g. specify the period of time (for example, seven years) that vendors must maintain the workpapers?[1]
   h. 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?
   i. 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?
   j. 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, SEC, Public Company Accounting Oversight Board (PCAOB), or regulatory independence guidance?
3. Does the outsourced internal audit arrangement maintain or improve the quality of the internal audit function and the bank's internal control?
4. Do key employees of the bank 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?
5. Is the scope of the outsourced work revised appropriately when the bank's environment, structure, activities, risk exposures, or systems change significantly?
6. Have the directors ensured that the outsourced internal audit activities are effectively managed by the bank?
7. Does the arrangement with the outsourcing vendor satisfy the independence standards described in the Policy Statement on the Internal Audit Function and Its Outsourcing and thereby preserve the independence of the internal audit function, whether or not the vendor is also the bank's independent public accountant?
8. Has the bank performed sufficient due diligence to satisfy itself of the vendor's competence before entering into the outsourcing arrangement, and are there adequate procedures for ensuring that the vendor maintains sufficient expertise to perform effectively throughout the arrangement?
9. Does the bank have a contingency plan to ensure continuity in audit coverage, especially for high-risk areas?

EXTERNAL AUDIT ENGAGEMENT LETTERS AND OTHER AUDIT AGREEMENTS

1. Does the bank's board of directors, audit committee, and senior management closely review all of the provisions in audit engagement letters or other audit work agreements before agreeing to sign them?
2. Does the bank's legal counsel carefully review audit engagement letters to ensure that those charged with engaging the external auditor make a fully informed decision?
3. Does the bank have any engagement letters for audits of financial statements, audits of internal control over financial reporting, or attestations on management's assessment of internal control that include unsafe and unsound provisions that—
   a. indemnify the external auditor against all claims made by third parties?
   b. hold harmless or release 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)?
   c. limit the remedies available to the client

1. 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.

financial institution (other than punitive damages)?

4. Has the bank agreed in any engagement letters or other audit work agreements 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. If so—
   a. has the bank's senior management carefully reviewed mandatory ADR and jury-trial provisions in engagement letters, as well as reviewed any agreements regarding rules of procedure, in order to fully comprehend the ramifications of any agreement to waive any available remedies?
   b. has the bank's senior management obtained written assurances that its insurance policies (for example, the bank's errors and omissions policies and directors' and officers' liability policies) will cover losses from claims that are precluded by limitation-of-liability provisions in audit engagement letters or other audit agreements?
5. Has the bank's senior management ensured that any mandatory ADR provisions in audit engagement letters are commercially reasonable and—
   a. apply equally to all parties?
   b. provide a fair process (e.g., neutral decision makers and appropriate hearing procedures)?
   c. are not imposed in a coercive manner?
6. Has the bank's board of directors, audit committee, or senior management documented their business rationale for agreeing to any provisions that limit their legal rights?

EXTERNAL AUDIT ACTIVITIES

1. When state, federal, or supervisory regulations or stock-exchange listing require an independent CPA audit, did the bank comply?
   a. If so, was the opinion rendered by the accounting firm unqualified?
   b. If not, has the auditor taken appropriate action to resolve any deficiencies?
2. Does the bank policy prohibit loans to its external auditor or the engagement of an external auditor who is a stockholder? If not, has the board considered the materiality of any existing transactions regarding the auditor's independence?
3. Has an external auditor been engaged to perform special reviews of specific departments or areas of the bank since the previous examination? If deficiencies were cited, have they been corrected?
4. Has the same public accounting firm been engaged for the prior two years? If not, obtain a reason for change.
5. Have management letters from the external auditors or other reports from consultants been presented to management since the last examination?
6. Do deficiencies in management letters receive appropriate attention?
7. Are the notes pertaining to the financial statements reviewed for any information that may allude to significant accounting or control problems?
8. Does the report of examination or the management letter submitted by the public accounting firm comprehensively define the scope of the examination conducted?

REGULATORY EXAMINATION ACTIVITIES

1. Does the internal audit department have access to the examination reports?
2. Does the internal audit department investigate the reasons for adverse comments and recommendations in the examination reports?
3. Does the internal audit department monitor the progress in dealing with these comments and recommendations?

The Federal Reserve System (System) maintains a long-standing policy that compels System employees, including examiners, to avoid any action that may result in an employee (or create the appearance that an employee) is—

- using his or her Federal Reserve position for private gain,
- giving preferential treatment to any person or institution,
- losing independence or impartiality, or
- making decisions outside of official channels.

Federal Reserve examiners are also subject to conflict-of-interest rules that are designed to ensure (1) both the objectivity and integrity of bank examinations and (2) that Federal Reserve examiners comply with criminal statutory prohibitions.

The conflict-of-interest rules are set forth in section 5 of the *Federal Reserve Administrative Manual* and in each Reserve Bank's uniform codes of conduct.

EXAMINER BORROWING RULES

A bank examiner is prohibited from accepting a loan or gratuity from any bank examined by the individual (18 USC 213). An officer, director, or employee of a bank is prohibited from making or granting any loan or gratuity to any examiner who examines or has authority to examine the bank (18 USC 212). These statutory provisions may also be applicable to a loan obtained by a System employee who has been issued a special, temporary, or ad hoc examiner credential. An examiner found to be in violation of these provisions can be—

- fined under title 18 of the U.S. Code (Crimes and Criminal Procedure), imprisoned not more than one year, or both;
- further fined a sum equal to the money loaned or gratuity given; and
- disqualified from holding office as an examiner.

On February 3, 2005, the director of the Board's Division of Banking Supervision and Regulation and the Board's general counsel, acting under delegated authority, approved changes to the System's examiner borrowing rules as a result of the Preserving Independence of Financial Institution Examinations Act of 2003 (18 USC 212–213). The act included provisions that liberalized examiner borrowing restrictions by providing narrow exceptions that enable bank examiners to obtain credit cards and certain home mortgage loans from a broader range of lenders. (See SR-05-2.)

Under the act, a Reserve Bank examiner may accept a credit card or a loan secured by a mortgage on the examiner's principal residence from an institution supervised by the Federal Reserve, as long as the examiner meets the financial requirements to obtain such credit or loan. The terms of the credit or loan cannot be more favorable than the terms that are generally offered to other borrowers. Federal Reserve policy, however, does not permit examiners to participate in the examination of any banking organization from which they have obtained home mortgage loans.

POST-EMPLOYMENT RESTRICTIONS FOR "SENIOR EXAMINERS"

On November 17, 2005, the federal bank regulatory agencies[1] adopted a rule (effective December 17, 2005) to implement the post-employment restriction found in the Intelligence Reform and Terrorism Prevention Act of 2004 (see 12 USC 1820).[2] (See the Board's rules at 12 CFR 263 and 264, as well as SR-05-26 and its attachments.) The restriction prohibits an examiner who served as a "senior examiner" for a depository institution or depository institution holding company for two or more months during the examiner's final twelve months of employment with a Reserve Bank from knowingly accepting compensation as an employee, an officer, a director, or a consultant from that depository institution or holding company, or from certain related entities.[3] *The rule is expected to affect a*

1. The Board of Governors of the Federal Reserve System (Board), the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision.

2. Pub. L. 108-458, 118 Stat. 3638, 3751–53 (December 17, 2004).

3. The Board's rule applies to a covered examiner who leaves the Federal Reserve's service after December 17, 2005. Because the statute has a one-year look-back provision, an

relatively small number of Federal Reserve examiners, primarily the ''central points of contact'' (CPC) or other examiners in functionally equivalent positions for the largest and most complex institutions. Table 1 summarizes how the restriction applies to ''senior examiners'' of the different types of organizations within the Federal Reserve's jurisdiction.

Definition of ''Senior Examiner''

For purposes of this rule, an officer or employee of the Federal Reserve is considered to be the ''senior examiner'' for a particular state member bank, bank holding company, or foreign bank if the individual meets all of the following criteria:

- The officer or employee has been authorized by the Board to conduct examinations or inspections on behalf of the Board.
- The officer or employee has been assigned continuing, broad, and lead responsibility for examining or inspecting that state member bank, bank holding company, or foreign bank.
- The officer's or employee's responsibilities for examining, inspecting, and supervising the state member bank, bank holding company, or foreign bank—
  - represent a substantial portion of the officer's or employee's assigned responsibilities and
  - require the officer or employee to interact routinely with officers or employees of the state member bank, bank holding company, or foreign bank or its respective affiliates.

The rule does not cover an examiner who performs only periodic, short-term examinations of a depository institution or holding company and who does not have ongoing, continuing responsibility for the institution or holding company. The rule also does not cover an examiner who spends a substantial portion of his or her time conducting or leading a targeted examination (such as a review of an institution's credit-risk management, information systems, or internal audit functions) and who does not have broad and lead responsibility for the overall examination program for the institution or holding company.

The restriction applies to a covered individual for one year after the individual terminates his or her employment with the Reserve Bank. If an examiner violates the one-year restriction, the statute requires the appropriate federal banking agency to seek an order of removal and industry-wide employment prohibition, a civil money penalty of up to $250,000, or both. In special circumstances, the Chairman of the Board of Governors may waive the restriction for the ''senior examiner'' of the Federal Reserve by certifying in writing that granting the individual a waiver of the restriction would not affect the integrity of the Federal Reserve's supervisory program.

---

examiner's responsibilities from as far back as December 17, 2004, may subject the "senior examiner" to the post-employment restriction.

Table 1—Summary of Prohibited Employment Based on Examination Responsibility

Examiner Responsibility	*Restriction*
If during two or more months of the last twelve months of service, the examiner serves as the ''senior examiner'' for a—	Then for one year after leaving the Reserve Bank, the ''senior examiner'' may not knowingly accept compensation as an employee, officer, director, or consultant from—
State member bank	• the state member bank (including any subsidiary of the state member bank) or • any company (including a bank holding company) that controls the state member bank.
Bank holding company	• the bank holding company or • any depository institution controlled by the bank holding company (including any subsidiary of the depository institution).
Foreign bank	• the foreign bank, • any U.S. branch or agency of the foreign bank, or • any U.S. depository institution controlled by the foreign bank (including any subsidiary of the depository institution).

Federal Reserve System Bank Watch List and Surveillance Programs

Effective date May 2006

Section 1020.1

The Federal Reserve System (the System) uses automated screening systems to conduct routine monitoring of the financial condition and performance of state member banks. These surveillance systems rely on Call Reports and other financial regulatory reports, as well as examination data, to identify institutions exhibiting financial deterioration or increased risk profiles. This surveillance process ensures that these banks receive timely supervisory attention and that examination resources can be directed to weak and potentially troubled banks to supplement on-site examinations.

System surveillance screens focus on many areas evaluated in the supervisory process, including capitalization, asset growth, loan quality, loan concentrations, interest-rate risk, and liquidity. In addition, the screens flag banks engaging in new or complex activities. The surveillance information helps identify weak or deteriorating banks and those with changing risk profiles.

Examiners also use the surveillance results in preexamination planning. For example, before an on-site review, the examiner will determine whether a bank is on the System's State Member Bank Watch List (the watch list) and if the bank has failed any surveillance monitoring screens. This information is useful in determining the type of examination scope (full, limited, or targeted) and staff resources that will be needed. The surveillance results can also be used to identify bank activities that may warrant a higher degree of review or focus during an on-site examination. Thus, the surveillance information helps examination and supervision staff plan and schedule more-forward-looking risk-focused examinations.

The surveillance program activities generally consist of the following three supervisory components:

1. *A set of System monitoring screens of financial data.* The process, referred to as ''screening,'' involves a routine monitoring of the financial condition, performance, and risk of banks.
2. *Analysis based on the watch list and other reports.* System staff use the watch list and other data derived from the surveillance process to flag outlier institutions, using measures that correspond to areas of supervisory concern. The monitoring screens and watch list are designed and used to spot trends and changes in an institution's financial condition and performance to determine if identified companies require further review.
3. *Corrective action and follow-up.* Reserve Bank follow-up action is performed for outlier institutions. The nature and extent of follow-up depend on current conditions at the identified bank. Actions range from completing a written analysis of the factors contributing to the outlier status to conducting an on-site examination. These efforts ensure that identified problems are monitored until they can be corrected or resolved.

SYSTEM BANK WATCH LIST PROGRAM

The State Member Bank Watch List Program, detailed in SR-06-2, ''Enhancements to the System's Off-Site Bank Surveillance Program,'' is the Federal Reserve's primary means for monitoring state member bank performance and condition between on-site examinations. The watch list is a record of banks that failed selected monitoring screens or ratings criteria. The watch list helps the Reserve Banks track and address troubled or potentially weak banks and identify common supervisory issues in the banks meeting watch list criteria. The program consists of five phases: (1) generating, reviewing, and modifying a watch list of banks meeting certain inclusion criteria; (2) analyzing the financial condition and risk profile of each bank on the final watch list and specifying the factors responsible for the bank's appearance on the watch list; (3) determining whether the safety-and-soundness examination schedule should be accelerated for those banks listed on the watch list; (4) preparing or updating a surveillance write-up for each bank listed on the watch list; and (5) developing a suitable supervisory response, including possible corrective action, that addresses identified problems.

The Watch List Program applies to all state member banks and includes both state member banks with known weaknesses and those with characteristics that could affect supervisory

assessments of the quality of bank management or of the overall safety and soundness of a bank. The program helps to ensure that weaknesses existing at supervised banks are being addressed appropriately and that potential emerging problems can be promptly identified in between regularly scheduled on-site safety-and-soundness examinations. State member banks are included on a watch list and require quarterly written analyses when they meet any of the following criteria:

- overall Supervision and Regulation Statistical Assessment of Bank Risk (SR-SABR) surveillance rating of 1D, 1F, 2D, or 2F
- CAMELS composite rating of 3 or worse
- Management or Risk Management component rating of 3 or worse
- composite rating in either of the worst two categories under the Trust, Information Technology, Consumer Compliance, or Community Reinvestment Act rating systems

Reserve Banks and Board staff may add state member banks to the watch list for reasons other than those listed above. For example, they may elect to include selected de novo banks, banks reporting rapid asset or loan growth or significant changes in business mix, and other institutions with financial characteristics that suggest the need for heightened off-site monitoring in between on-site examinations.

SR-SABR Model

The SR-SABR model assigns a two-component surveillance rating to each bank. The first component is the current composite CAMELS rating assigned to the bank. The second component is a letter (A, B, C, D, or F), reflecting the model's assessment of the relative strength or weakness of a bank compared with other institutions within the same CAMELS rating category.[1] An SR-SABR rating that includes an "A" denotes a bank with particularly strong financial and supervisory indicators compared with other banks within its CAMELS rating category. An SR-SABR rating including an "F" indicates that a bank is reporting poor financial results or showing other signs of significant weakness compared with similarly rated banks. For example, a 1A rating signifies a 1-rated bank that reports strong financial and supervisory indicators when compared with all 1- and 2-rated banks, while a 1F indicates that, while the bank currently maintains the strongest possible composite CAMELS rating, its financial or other supervisory indicators place it among the weakest of the banks currently rated either 1 or 2. SR-SABR ratings that include a "B" generally correspond to banks with financial and supervisory measures that are comparable to most banks in the CAMELS rating category. Those with a "C" have weaker measures than those of most other banks in their CAMELS rating category, and those with a "D" have significantly weaker financial or supervisory measures compared with other banks in their rating category.

Three separate econometric models contribute to SR-SABR surveillance ratings. Two of the models estimate the probability of an adverse supervisory rating change for a bank if it was examined within the next quarter. The first estimates the probability of an adverse rating change for banks currently rated CAMELS 1 or 2. The second estimates the probability of an adverse rating change for banks currently rated 3, 4, or 5.[2] Together, these models are used to assign an "adverse change" rating. They utilize seven financial variables computed using Call Report data and seven supervisory variables that have been statistically significant in explaining adverse ratings assigned over the past three years. The third model is retained from the System to Estimate Examination Ratings (SEER) framework and estimates the probability that a bank will fail or become critically undercapitalized within the next two years. This model is referred to as the "viability" model and includes 11 financial variables computed using Call Report data. The model was estimated and developed based on the financial results from the large group of banks that failed in the late 1980s and early 1990s.

Quarterly Watch List Procedures

Board staff will distribute a preliminary quarterly watch list to surveillance contacts at each

1. For banks currently rated 1 or 2, "CAMELS rating category" refers to all banks with satisfactory (1 or 2) CAMELS ratings. Banks with less than satisfactory CAMELS ratings are compared only with other banks that have the same CAMELS rating.

2. For 5-rated banks, an adverse rating change is defined as the continuation of the current rating.

Reserve Bank upon the finalization of quarterly Call Report processing. To assist examiners and analysts in interpreting SR-SABR model results, Board staff will also distribute SR-SABR Schedule of Risk Factors (SRFs) reports. The SRFs highlight financial ratios that cause the model to flag a bank as particularly strong or weak. These reports also include peer statistics to highlight the relative position of a bank compared with other institutions that have similar CAMELS composite ratings. In addition, supplemental monitoring screens will be distributed to assist in analyzing watch list banks and in identifying other banks that may require additional supervisory attention.

Upon notification from Board staff that quarterly surveillance materials are ready for review, Reserve Banks should perform the following procedures:

- *Review and modify the watch list.* Review the preliminary watch list and add any other state member banks from their districts that have significant safety-and-soundness weaknesses. For each bank to be added, the Reserve Bank should submit the name, ID RSSD number, location, asset size, and the reasons for its inclusion on the watch list by e-mail to the manager of the Surveillance, Financial Trends, and Analysis Section at the Board within five business days of receiving the preliminary watch list. Reserve Banks also may recommend removal of banks that they previously had added to the watch list and that no longer appear to warrant watch list status. In these cases, the Reserve Bank should also provide a brief written rationale to Board staff for removing any banks from the watch list. Ten days after the distribution of the draft, the watch list will be deemed final, and the time frame for completing all follow-up work will commence.
- *Assess the financial condition and risk profile of each final watch list bank.* Reserve Banks should review each final watch list bank in their Districts to assess the bank's financial condition and risk profile. Reserve Banks should consider recent examination findings for the bank and its affiliates, relevant information included in correspondence between the bank and the Reserve Bank, and other outside sources of information. Reserve Banks also should use all appropriate surveillance tools in evaluating each bank, including the Uniform Bank Performance Report, Bank Holding Company Performance Reports, and results of the System Bank Monitoring Screens and the System BHC Monitoring Screens.
- *Determine whether the safety-and-soundness examination schedule should be accelerated for each watch list bank.* In cases where substantial deterioration in a bank's financial condition is evident or where a bank's risk profile has increased significantly, Reserve Banks should commence an on-site review of the bank no later than 60 days after the release of the final watch list. Unless an on-site examination has been completed within the last six months or the Reserve Bank can document that SR-SABR results do not reflect material safety-and-soundness concerns, Reserve Banks should generally accelerate examinations when a state member bank is assigned an SR-SABR rating of 1F, 2F, or 3F. The scope of on-site reviews conducted for watch list banks may vary, depending on the risk factors present and knowledge about the bank and its management. In some cases, discussing the issues with management may suffice; in others, a full-scope safety-and-soundness examination may be necessary.
- *Prepare surveillance write-ups for each watch list bank.* No more than 30 days after receiving the quarter's final watch list, Reserve Banks should document conclusions on the watch list banks in a write-up posted to the System's Central Data and Text Repository (CDTR) using the Banking Organization National Desktop (BOND) application.[3] Each write-up should be posted as a "State Member Bank Watch List Write-Up" and assigned an "as of" date that corresponds to the quarterly surveillance cycle. The write-ups should—
  - briefly summarize the cause for a bank's appearance on the watch list and assess whether it poses risks to the safety and soundness of the bank;

3. In general, Reserve Banks should create a separate quarterly watch list document for each state member bank included on the watch list. However, for bank subsidiaries of the largest banking organizations, which are subject to continuous supervision and already require separate quarterly written analyses, the factors required for a quarterly watch list write-up, if applicable, may be addressed within the standard quarterly documentation posted in the CDTR and BOND. Reserve Bank surveillance contacts, however, should notify the manager of the Surveillance, Financial Trends, and Analysis section of the specific CDTR documents that address these requirements.

— detail the supervisory actions that have been taken in response to safety-and-soundness concerns;
— describe bank management's response to safety-and-soundness concerns;
— address whether the current CAMELS rating accurately reflects the bank's condition, considering adverse SR-SABR results when applicable;
— assess whether the timing of the next safety-and-soundness examination should be accelerated; and
— describe the Reserve Bank's plans for addressing any safety-and-soundness issues over the next quarter.

For state member banks that have been included on the watch list in the prior quarter, write-ups should focus on new developments or changes in the condition or performance of the bank. Key background information, however, should be carried forward so that the write-up serves as a stand-alone summary document of the bank's current condition and prospects for improvement.

1. To identify major changes in the financial condition of the bank between examinations.
2. To assist in determining the scope of the examination and the priority of work to be performed.
3. To check the validity of the data being reported by the bank.
4. To investigate areas where an in-depth review is indicated.

1. Obtain any surveillance screening reports, such as the watch list and Federal Reserve System monitoring screens, or other analysis reports prepared by the Reserve Bank or Board that have been generated for the bank.
2. Review the reports obtained in step 1 and discuss with surveillance staff, if necessary, for clarification or for further background information.
3. If a pre-examination analysis has not been prepared, create one from information contained in the bank performance report, current call report, and previous examination report. This analysis should be considered when determining the scope of the examination, and when making staffing decisions.
4. Follow up on unusual aspects revealed in the surveillance screening reports, in analysis reports, or on newly obtained data significantly different from prior information.
5. Perform validity checks necessary to ensure the quality of reported data. This would include such normal examination procedures as validating call report information and confirming the accuracy and soundness of past-due and accrual accounting practices.

INTRODUCTION

Workpapers are the written documentation of the procedures followed and the conclusions reached during the examination of a bank. Accordingly, they include, but are not necessarily limited to, examination procedures and verifications, memoranda, schedules, questionnaires, checklists, abstracts of bank documents and analyses prepared or obtained by examiners.

The definition of workpapers, their purpose, and their quality and organization are important because the workpapers as a whole should support the information and conclusions contained in the related report of examination. The primary purposes of workpapers are to—

- organize the material assembled during an examination to facilitate review and future reference.
- aid the examiner in efficiently conducting the examination.
- document the policies, practices, procedures and internal controls of the bank.
- provide written support of the examination and audit procedures performed during the examination.
- document the results of testing and formalize the examiner's conclusions.
- substantiate the assertions of fact or opinion contained in the report of examination.

They also are useful as—

- a tool for the examiner-in-charge to use in planning, directing, and coordinating the work of the assistants.
- a means of evaluating the quality of the work performed.
- a guide in estimating future personnel and time requirements.
- a record of the procedures used by the bank to assemble data for reports to the Board of Governors of the Federal Reserve System.
- a guide to assist in the direction of subsequent examinations, inquiries and studies.

The initial step in preparing workpapers is to review, where available, the applicable sections of supporting data prepared during the prior examination. When reviewing prior workpapers, the examiner should consider the data prepared in each area for—

- information that is of a continuing or permanent nature.
- guidance in preparation of workpapers for the current examination.
- an indication of changes or inconsistencies in accounting procedures or methods of their application since the last examination.

Accumulation of relevant documentation consistent with prior examinations, however, is often insufficient. Workpapers should be prepared in a manner designed to facilitate an objective review, should be organized to support an examiner's current findings and should document the scope of the current examination. Minimum content necessary for each section of workpapers includes:

Source of Information—This is important, not only in identifying the bank, but also in identifying the preparer. In subsequent examinations, the preparer should be able to readily determine the bank personnel from whom the information was obtained during the previous examination as well as the examiner who prepared the workpapers. Accordingly, each workpaper should include—

- bank name and subdivision thereof, either functional or financial.
- statement of title or purpose of the specific analysis or schedule.
- specific identification of dates, examination date and work performance date.
- initials of preparer and initials indicating review by the examiner designated to perform that function. Although appropriate use may be made of initials, the full names and initials of all examiners should appear on a time and planning summary or on an attachment to the file to facilitate future identification.
- name and title of person, or description of records, that provided the information needed to complete the workpaper.
- an index number identifying the workpaper and facilitating organization of the workpaper files.

Scope of Work—This includes an indication of the nature, timing and extent of testing in application of examination and audit procedures. It also includes the examiner's evaluation of and reliance on internal and external audit

procedures and compliance testing of internal controls. To the extent that this information is contained in other workpapers, such as an examination procedure or a questionnaire, a reference to the appropriate workpaper will be sufficient.

Conclusions—The examiner should develop conclusions, in accordance with the examination objectives, with respect to the information obtained, documentation provided and the results of the examination and audit procedures performed. Such conclusions provide the basis for information contained in the report of examination.

To develop workpapers that have the qualities of clarity, completeness and conciseness, adequate planning and organization of content are essential. Therefore, before the workpaper is prepared, the examiner should determine the following:

- What examination objective will be satisfied by preparing the analysis or workpaper?
- Can preparation of the analysis be avoided by testing the bank's records and indicating the nature and extent of testing in an examination or an audit procedure or by comment on a related schedule or another supporting document?
- Is the analysis necessary to support the information in the report of examination?

Subsequent to the determination that an analysis is required, but before initiating preparation, the examiner should decide if—

- previous examination analyses can be adapted and carried forward to the current examination.
- the analysis can be prepared by an internal auditor or other bank personnel.
- the format of the analysis may be designed in a manner to facilitate its use in future examinations.

Once it has been determined that preparation of an analysis is required, the examiner should consider the following techniques that promote clarity of workpaper preparation:

- Restrict writing to only one side of the paper.
- Use a standard size sheet of paper large enough to avoid overcrowding.
- Condense information for simplicity.

Frequently, time can be saved by carrying forward workpapers from one examination to the next. Thus, when laying out an analysis that might be repeated in future examinations, the examiner should arrange it in a manner to facilitate future use. For example, extra columns may be left blank within an account analysis displaying little activity for insertion of transaction information during future examinations. In such a situation, appropriate space (boxes and column headings) should be provided for the signature or initials of the preparer and reviewer during each examination. When a workpaper is removed from one examination file and carried forward, a notation should be made in the file from which the paper is extracted. This is important in the event workpapers applicable to a particular examination are needed several years after the completion of the examination.

INITIAL PREPARATION BY OTHERS

Although all items included in the report of examination should be supported by workpapers, their preparation may not always require original work by the examiner. Frequently, arrangements can be made for bank personnel, including internal auditors, to prepare workpapers for examination use or to make available papers prepared by them as part of their regular duties. Examples include outstanding checklists, lists of outstanding certificates of deposit, schedules of employee borrowings, and debt maturity schedules. The extent to which examiners can utilize analyses and data prepared by bank personnel increases the efficiency with which examination procedures are completed.

As part of the initial examination planning process, arrangements should be made with appropriate bank management for the timely completion of bank-prepared data and information. The coordinating bank officer(s) must understand what information is being requested and why it is being requested, in order to avoid confusion and unnecessary regulatory burden. Arrangements, however, may have to be made for the bank to supply supporting details or other schedules or items to comply with the requests.

Upon receipt of bank-prepared analyses, an examiner should review the documents for over-

all completeness and note the date of receipt. This facilitates future planning and provides a ready reference as to which analyses have been received from the bank at any given point during the examination. Also, all bank-prepared workpapers should be tested and the nature and extent of testing performed by the examiner should be indicated on the papers.

INITIAL APPROACH IN WORKPAPER PREPARATION

The initial approach in preparing workpapers that support balances in the statement of condition is quantitative. In using this approach, the examiner obtains an analysis of the composition of the account balance as of the examination date. This inventory of the composition may be represented by a trial balance of loans, a listing of outstanding official checks, a listing of individual deposit accounts, or other similar items. Only after determining the composition and insuring that the total agrees with the bank's records is the examiner in a position to perform examination procedures and to arrive at a conclusion about the overall quality of the items comprising the balance.

For certain analyses, however, it is preferable to include account activity (transactions) in the workpapers. Typical examples of such analyses are those of bank premises and equipment and of reserve for possible loan losses. The format for reserve for possible loan losses should include beginning balances (prior examination ending balances), provisions for loan losses, collections, charge-offs, other transactions (transfers to/from undivided profits) and ending balances as of the examination date.

CONTROL AND REVIEW

All examiners assigned to an examination should insure that workpapers are controlled at all times while the examination is in progress. For example, when in the bank's offices, the workpapers should be secured at night and safeguarded during the lunch hour or at other times when no examining personnel are present in the immediate vicinity. It is essential to completely control confidential information provided by the bank. In addition, information relating to the extent of tests and similar details of examination procedures should not be made available to bank employees.

In cases where customary examination practices are not practical, alternative procedures and the extent to which they are applied should be documented. The need for completeness requires that there be no open items, unfinished operations or unanswered questions in the workpapers at the conclusion of the examination.

The clarity of workpapers should be such that an examiner or Federal Reserve official unfamiliar with the work could readily understand it. Handwritten commentaries should be legible, concise and should support the examiner's conclusions. Descriptions of work done, notations of conferences with bankers, conclusions reached and explanations of symbols used should be free from ambiguity or obscurity. Excessive use of symbols usually can be avoided by expanding a comment to include the nature and extent of work performed instead of using separate symbols for each portion of the work performed. In addition, instructions to assisting personnel concerning standards or workpaper content are necessary to ensure that they will meet the quality standards of the Federal Reserve. When workpapers have the necessary qualities of completeness, clarity, conciseness and neatness, a qualified reviewer may easily determine their relative value in support of conclusions and objectives reached. Incomplete, unclear or vague workpapers should, and usually will, lead a reviewer to the conclusion that the examination has not been adequately performed.

REVIEW PROCEDURES

Experienced personnel must review all workpapers prepared during an examination. Usually that review is performed by the examiner-in-charge, although in some cases, the examiner-in-charge may designate other experienced personnel to perform an initial review. An overall review is then performed by the examiner-in-charge. The two primary purposes of a review of workpapers by senior personnel are to determine that the work is adequate given the circumstances, and to ensure that the record is sufficient to support the conclusions reached in the report of examination. The timely review of workpapers and subsequent discussion of them with the individual who prepared them also is one of the more effective procedures for on-the-job training.

Normally, the review should be performed as soon as practicable after the completion of each work area. This review ideally occurs at the bank's office so that if the need for obtaining additional information arises or additional work is required the matter can be promptly attended to with minimum loss of efficiency.

When the review of workpapers is completed, the reviewer should sign or initial the applicable documents. Although all workpapers should be reviewed, the depth and degree of detail depends on factors such as:

- The nature of the work and its relative importance to the overall examination objectives.
- The extent to which the reviewer has been associated with the area during the examination.
- The experience of the examiners who have carried out the various operations.

Professional judgment must be exercised throughout the review process.

ORGANIZATION OF WORKPAPER FILES

Administration of an examination includes—

- organizing the workpaper files.
- delegating authority for completion of all applicable workpaper sections.
- reviewing and assembling the completed workpapers.

To ensure efficiency in locating information contained in the workpapers and completion of all necessary procedures, workpapers should be filed and indexed in a standard manner.

FILES

The file provides the organizational vehicle to assemble workpapers applicable to specific areas of the examination. Files might include detailed workpapers related to—

- management appraisal.
- overall conclusions about the condition of the bank.
- cash accounts.
- investments.
- loans.
- reserve for possible loan losses.
- bank premises and equipment.
- other assets.
- deposits.
- other liabilities.
- capital accounts and dividends.

Each individual file would normally include—

- related examination and audit procedures.
- detailed information and other documentation necessary to indicate the specific procedures performed, the extent of such procedures and the examiner's conclusions for the specific area.
- a summary, in comparative form, of the supporting general ledger balances with appropriate cross-references.

Judgment is required as to what the file should include on any specific examination. Lengthy documents should be summarized or highlighted (underlined) so that the examiner who is performing the work in the related area can readily locate the important provisions, without having to read the entire document. It also may be desirable to have a complete copy of the document in the file to support the summaries or answer questions of a specific legal nature.

Examples of documents that might be contained in the files are—

- a brief history and organization of the bank.
- organization charts of applicable departments within the bank.
- copies of, or excerpts from, the charter and bylaws.
- copies of capital stock certificates, debentures agreements and lease agreements.
- excerpts from minutes or contracts that are of interest beyond the current year.
- a chart of accounts and an accounting manual, if available, supplemented by descriptions of unique accounts and unusual accounting methods.
- lists of names and titles of the board of directors, important committees and relevant departmental personnel.

Indexing and Cross-Referencing

To promote efficiency and help ensure that all

applicable areas of an examination have been considered and documented, the use of an indexing system aids in the organization of workpaper files. A general outline or index including all examination areas provides a basis for organization to which a numbering or other sequential system can be assigned and applied to each workpaper file.

When all workpapers pertinent to a specific area of the examination have been completed, a cover sheet listing the contents of each file should be attached to the front to provide a permanent record for reference. This permits not only efficient location of a set of workpapers pertinent to a specific area of the examination (for example, cash or commercial loans), but also facilitates the location of a specific analysis (or other document) within the set.

Amounts or other pertinent information appearing in more than one place in the workpapers should be cross-referenced between the analyses. A notation on the index, including appropriate cross-referencing of those items removed or filed elsewhere, facilitates location of specific data and records and also helps to prevent inadvertent loss of documents. An example is the cross-referencing of net charge-offs obtained in the review of the reserve for possible loan losses to the amount approved in the board of director's minutes. Proper cross-referencing is important because it—

- serves as a means of locating work performed for a particular account or group of accounts.
- identifies the source of supporting amounts in a particular analysis.
- facilitates the review of the workpapers.
- helps in following the workpapers during the succeeding examination.

WORKPAPER RETENTION

Examiners should retain on a readily available basis those workpapers from—

- the most recent full-scope Federal Reserve examination.
- the most recent general EDP examination.
- examinations of banks requiring or recommended for more than normal or special supervisory attention (composite rating of 3, 4 or 5; consumer compliance rating of 3, 4 or 5; EDP departments rated 4 or 5; or those subject to administrative action such as civil money penalties) until such banks are no longer the subject of such scrutiny.
- examinations disclosing conditions that may lead eventually to more than normal or special supervisory attention, as described above, until the supporting workpapers are no longer appropriate.
- examinations disclosing conditions that lead, or may eventually lead, to a criminal referral or criminal investigation.

These guidelines are the minimum required retention period for workpapers; longer retention periods may be set by individual Reserve Banks.