←
INTRODUCTION

Internal controls include the policies and procedures that financial institutions establish to reduce risks and ensure they meet operating, reporting, and compliance objectives. The board of directors is responsible for ensuring internal control programs operate effectively. Their oversight responsibilities cannot be delegated to others within the institution or to outside parties. The board may delegate operational activities to others; however, the board must ensure effective internal control programs are established and periodically modified in response to changes in laws, regulations, asset size, organizational complexity, etc.

Internal control programs should be designed to ensure organizations operate effectively, safeguard assets, produce reliable financial records, and comply with applicable laws and regulations. Internal control programs should address five key components:

- Control environments,
- Risk assessments,
- Control activities,
- Information and communication, and
- Monitoring.

These components must function effectively for institutions to achieve internal control objectives. This overview of internal control is described further in a report by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) titled *Internal Control-Integrated Framework*. Institutions are encouraged to evaluate their internal control program against this COSO framework.

←
INTERNAL CONTROL SYSTEMS

Part 364 of the FDIC Rules and Regulations establishes safety and soundness standards that apply to insured state nonmember banks and state-licensed, insured branches of foreign banks. Appendix A to Part 364 includes, among other things, general standards for internal controls, information systems, and audit programs. The standards require all financial institutions to have controls, systems, and programs appropriate for their size and the nature, scope, and risk of their activities. Internal controls and information systems should ensure:

- An organizational structure that defines clear lines of authority and responsibilities for monitoring adherence to established policies;
- Effective risk assessments;
- Timely and accurate financial, operational, and regulatory reports;
- Adequate procedures to safeguard and manage assets; and
- Compliance with applicable laws and regulations.

Many internal controls are programmed directly into software applications as part of data input, processing, or output routines. Other controls involve procedural activities standardized in an institution's policies. The relative importance of an individual control, or lack thereof, must be viewed in the context of other controls. Every bank is unique, and one set of internal procedures cannot be prescribed for all institutions. However, all internal control programs should include effective control environments, risk assessments, control activities, information systems, and monitoring programs.

If examiners determine internal routines or controls are deficient, they should discuss the deficiencies with the chief executive officer and the board of directors, and include appropriate comments in the report of examination (ROE).

Key Control System Components

Control Environment

The control environment begins with a bank's board of directors and senior management. They are responsible for developing effective internal control systems and ensuring all personnel understand and respect the importance of internal controls. Control systems should be designed to provide reasonable assurance that appropriately implemented internal controls will prevent or detect:

- Materially inaccurate, incomplete, or unauthorized transactions;
- Deficiencies in the safeguarding of assets;
- Unreliable financial and regulatory reporting; and
- Deviations from laws, regulations, and internal policies.

Risk Assessments

Risk assessments require proper identification, measurement, analysis, and documentation of significant business activities, associated risks, and existing controls. Financial risk assessments focus on identifying control weaknesses and material errors in financial statements such as incomplete, inaccurate, or unauthorized transactions. Risk assessments are conducted in order to identify, measure, and prioritize risks so that attention is placed first on areas of greatest importance. Risk assessments should analyze threats to all significant

business lines, the sufficiency of mitigating controls, and any residual risk exposures. The results of all assessments should be appropriately reported, and risk assessment methodologies should be updated regularly to reflect changes in business activities, work processes, or internal controls.

Control Activities

Control activities include the policies and procedures institutions establish to manage risks and ensure pre-defined control objectives are met. Preventative controls are designed to deter the occurrence of an undesirable event. Detective controls are designed to identify operational weaknesses and help effect corrective actions. Control activities should cover all key areas of an organization and address items such as organizational structures, committee compositions and authority levels, officer approval levels, access controls (physical and electronic), audit programs, monitoring procedures, remedial actions, and reporting mechanisms.

Information and Communication

Reliable information and effective communication are essential for maintaining control over an organization's activities. Information about organizational risks, controls, and performance must be quickly communicated to those who need it. Technology systems and organizational procedures should facilitate the effective distribution of reliable operational, financial, and compliance-related reports. Clearly defined procedures should be developed that make it easy for individuals to report risks, errors, or fraud through formal and informal means. The procedures should include appropriate mechanisms for communicating, as needed, with external parties such as customers, regulators, shareholders, and investors.

Monitoring

Internal control systems must be monitored to ensure they operate effectively. Monitoring may consist of periodic control reviews specifically designed to ensure the sufficiency of key program components, such as risk assessments, control activities, and reporting mechanisms. Monitoring the effectiveness of a control system may also involve ongoing reviews of routine activities. The effectiveness of a periodic review program is enhanced when people with appropriate skills and authority are placed in key monitoring roles.

Control Standards

The control environment begins with the board of directors, which must establish appropriate control standards. The board of directors or an audit committee, preferably consisting entirely of outside directors (directors independent of operational duties), must monitor adherence to established directives.

Boards should establish policy standards that address issue such as decision-making authorities, segregation of duties, employee qualifications, and operating and recording functions. Key internal controls are described below.

Director Approvals

The board of directors should establish limits for all significant matters (such as lending and investment authorities) delegated to relevant committees and officers. Management should regularly provide financial and operational reports to the board, including standardized reports that detail policy exceptions, new loans, past due credits, concentrations, overdrafts, security transactions, etc. The board or a designated board committee should periodically review all authority levels and material actions. The key control objective is that the board is regularly informed of all significant matters.

Sound Personnel Policies

Sound personnel policies are critical components of effective control programs. The policies should require boards and officers to check employment references, hire qualified officers and competent employees, use ongoing training programs, and conduct periodic performance reviews.

Management should check the credit and previous employment references of prospective employees. The FBI is available to check the fingerprints of current and prospective employees and to supply institutions with criminal records, if any, of those whose fingerprints are submitted. Some insurance companies that write bankers' blanket bonds also offer assistance in screening officers and employees.

Pursuant to Section 19 of the Federal Deposit Insurance Act (FDI Act), the FDIC's written consent is needed in order for individuals to serve in an insured bank as a director, officer, or employee if they have been convicted of a criminal offense involving dishonesty, breach of trust, or money laundering.

Segregation of Duties

The possibility of fraud diminishes significantly when two or more people are involved in processing a transaction. A segregation of duties occurs when two or more individuals are required to complete a transaction. The segregation of duties allows one person's work to verify that transactions initiated by another employee are properly authorized,

recorded, and settled. When establishing segregation-of-duty standards, management should assign responsibilities so that one person cannot dominate a transaction from inception to completion. For example, a loan officer should not perform more than one of the following tasks: make a loan, disburse loan proceeds, or accept loan payments. Individuals having authority to sign official checks should not reconcile official check ledgers or correspondent accounts, and personnel that originate transactions should not reconcile the entries to the general ledger. Additionally, information technology (IT) personnel should not initiate and process transactions, or correct data errors unless corrections are required to complete timely processing. In this situation, corrections should be pre-authorized, when possible, and authorized personnel should review and approve all corrections as soon as practical after the corrections are processed, regardless of any pre-authorizations.

Automated controls that act similar to manual segregation-of-duty controls can be written into software programs. For example, automated holds can be placed on customer accounts requiring special attention, such as dormant accounts or accounts with large uncollected funds. An automated hold allows tellers or customer service representatives to access an account for a customer, but requires the approval of a second person to authorize a transaction. In addition, certain modifications of data, such as master file changes, should require action from two authorized people before data is altered. When a hold on an account is added or removed, or when an action requiring supervisory approval occurs, exception reports should be automatically printed and reviewed by a designated person who is not involved with the activity. When properly designed, automated control methods are generally considered superior to manual procedures.

Joint Custody

Joint custody (a.k.a. *dual control*) refers to a procedure where two or more persons are equally accountable for the physical protection of items or records. For example, two keys or split combinations or passwords, under the separate control of different individuals, must be used in order to obtain access to vaults, files, or other storage devices. These custodial responsibilities should be clearly assigned and communicated to all affected employees. For the system to be effective, persons exercising control must guard their key, combination, or password carefully. If this is done, only collusion can bypass this control feature. Examples of items that should be under joint custody include reserve cash, negotiable collateral, certificated securities, trust assets, safekeeping items, reserve supplies of official checks, unissued electronic debit or credit cards, and unissued traveler's checks. Other examples include spare locks, keys, or combinations to night depositories, automated teller machines, safe deposit boxes, and tellers' cash drawers.

Vacation Policies

Banks should have a policy that requires all officers and employees to be absent from their duties for an uninterrupted period of not less than two consecutive weeks. Absence can be in the form of vacation, rotation of duties, or a combination of both activities. Such policies are highly effective in preventing embezzlements, which usually require a perpetrator's ongoing presence to manipulate records, respond to inquiries, and otherwise prevent detection. The benefits of such policies are substantially, if not totally, eroded if the duties normally performed by an individual are not assumed by someone else.

Where a bank's policies do not conform to the two-week recommended absence, examiners should discuss the benefits of this control with senior management and the board of directors and encourage them to annually review and approve the bank's actual policy and any exceptions. In cases where a two-week absent-from-duty policy is not in place, the institution should establish appropriate compensating controls that are strictly enforced. Any significant deficiencies in an institution's vacation policy or compensating controls should be discussed in the ROE and reflected in the Management component of the Uniform Financial Institutions Rating System (UFIRS).

Note: Management should consider suspending or restricting an individual's normal IT access rights during periods of prolonged absence, especially for employees with remote or high-level access rights. At a minimum, management should consider monitoring and reporting remote access during periods of prolonged absence.

Rotation of Personnel

Personnel rotations can provide effective internal controls and be a valuable part of overall training and business-continuity programs. The rotations should be planned by auditors and senior officers to ensure maximum effectiveness, but should not be announced ahead of time to the involved personnel. The rotations should be of sufficient duration to permit disclosure of irregularities due to error or fraud.

Pre-numbered Documents

Financial institutions should use sequentially numbered instruments wherever possible for items such as official checks and unissued stock certificates. In addition, institutions should maintain board meeting minutes on pre-numbered pages. Pre-numbered documents aid in proving,

reconciling, and controlling used and unused items. Number controls should be monitored by a person who is detached from the particular operation; and unissued, pre-numbered instruments should be maintained under joint custody.

Cash Controls

Institutions should provide tellers with a separate cash drawer to which they have sole access. Common cash funds should not be used. An inability to fix responsibility in the event of a discrepancy could unnecessarily embarrass an employee or result in improper termination. Random cash drawer audits are also a fundamental control process.

Reporting Irregularities and Shortages

Management should develop procedures for the prompt reporting and investigation of irregularities and identified shortages. The results of investigations should be regularly reported to management and internal auditors, and when appropriate to fidelity insurers, regulators, and law enforcement agencies.

Business Continuity Plans

Business continuity planning requires banks to consider the impact of disruptions from natural disasters, technical problems, malicious activities (such as cyber attacks), pandemic incidents, etc. Directors and senior managers must develop business continuity plans to protect physical assets, safeguard financial records, and minimize operational interruptions.

Management should develop continuity plans for all significant operational areas based on the potential impact and probable occurrence of business disruptions. Disruptions include those with a high probability of occurrence and low impact to an institution, such as brief power interruptions, and to disruptions with a lower probability of occurrence but higher impact to an institution, such as tornadoes.

Business continuity plans should define key roles, responsibilities, and succession plans for various operational areas. Independent internal or external auditors should review the adequacy of the plans at least annually. Management should establish adequate training programs, periodically test the continuity plans, and report the test results and any recommendations for improvements to the board.

For additional details, refer to the FFIEC IT Examination Handbook titled Business Continuity Planning.

Accounting Systems

Efficient banking operations cannot be conducted without recordkeeping systems that generate accurate and reliable information and reports. Such systems are necessary to keep directors well informed and help officers manage effectively. Properly documented records are also necessary for meeting the needs of customers, shareholders, supervisory agencies, tax authorities, and courts of law.

Accounting systems should be designed to facilitate the preparation of internal reports that correspond with the responsibilities of individual supervisors and key employees. Records should be updated daily and reflect each day's activities separately from other days. Subsidiary records, such as those pertaining to deposits, loans, and securities, should balance with general ledger accounts.

While it is expected that records and systems will differ between banks, the books of every institution should be kept in accordance with well-established accounting and banking principles. In each instance, a bank's records and accounts should accurately reflect financial conditions and operating results. The following characteristics should be present in all accounting systems.

Audit Trail

Recordkeeping systems should be designed to enable the tracing of any transaction as it passes through accounts. Some of the more common recordkeeping deficiencies encountered during examinations include:

- General ledger entries are outdated or fail to contain adequate transaction descriptions;
- Customer loan records are incorrect, incomplete, or nonexistent;
- Cash item, overdraft, and suspense account records are deficient;
- Teller cash records are inadequately detailed;
- Security registers (electronic or manual) do not include all necessary information;
- Correspondent bank account reconcilements are outdated, lack complete descriptions, or fail to reflect the status of outstanding items;
- Account overage or shortage descriptions lack sufficient details;
- Letters of credit or other contingent liability records are inadequate; and
- Inter-office or intra-branch accounts are not properly controlled or monitored.

Accounting Manual

The uniform handling of monetary transactions is essential to the production of reliable financial reports. Management should establish accounting manuals and data processing guides that help employees consistently process and record transactions. Data processing guides are often provided by a servicer and supplemented by procedures written by bank personnel. The guides normally include instructions for compiling and reconciling source documents (such as checks and transaction tickets), instructions for processing the documents internally or transmitting them to a servicer for processing, and instructions for distributing output reports. Many systems allow employees to image source documents and transmit electronic files to a servicer for final posting. Regardless of the method used to process financial transactions, banks should have clear instructions for recording transactions and controlling the movement of documents and data between customers, the bank, and data processors.

←

AUDIT

Internal control and internal audit are related, but separate concepts. Internal control involves the systems, policies, and procedures that institutions design to control risks, safeguard assets, and achieve objectives. Internal audits help directors and officers evaluate the adequacy of internal control systems by providing independent assessments of internal controls, bank activities, and information systems.

Appropriately structured and monitored audit programs substantially lessen financial and operational risks, and all banks should adopt adequate audit programs. Ideally, such programs include ongoing internal audits and periodic external audits.

Internal Audit

The board of directors and senior management are responsible for ensuring internal control systems operate effectively. Internal audits provide a systematic way for institutions to assess the effectiveness of risk-management and internal-control processes. When properly structured and conducted, internal audits provide vital information about risks and controls so management can promptly address any identified weaknesses.

When examiners identify weaknesses in internal auditing programs, they should discuss their concerns with management and the board and include appropriate recommendations in the ROE.

General Standards

As noted previously, Appendix A to Part 364 of the FDIC Rules and Regulations includes general standards for internal controls, information systems, and audit programs. Internal audit programs should be appropriate for the size of an institution and the nature and scope of its activities, and provide for:

- Adequate monitoring of the internal control system;
- Independence and objectivity;
- Qualified personnel;
- Adequate testing and review of information systems;
- Adequate documentation of tests, findings, and corrective actions;
- Verification and review of management's actions to address material weaknesses; and
- Review by the audit committee or board of directors of the effectiveness of the internal audit function.

The 2003 Interagency Policy Statement on the Internal Audit Function and its Outsourcing discusses:

- Board and management responsibilities,
- Key characteristics of the internal audit function,
- Considerations at small institutions,
- Outsourcing arrangements,
- Independence considerations when external auditors also provide internal audit services,
- Independence requirements relating to public and non-public companies,
- Annual audit and reporting requirements based on an institution's size, and
- Examiner reviews of internal audit functions and related matters.

As previously noted, directors and senior management should have reasonable assurance that the internal control system prevents or detects inaccurate, incomplete, or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial reporting; and deviations from laws, regulations, and internal policies.

To ensure the internal audit program is appropriate for the institution's current and planned activities, 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 provide criteria to address independence, professional proficiency, scope of work, performance of audit work, management of internal audits, and quality assurance reviews. Furthermore, directors and senior management should ensure the internal audit program adequately reflects key functional characteristics regarding

organizational structure; management, staffing, and audit quality; scope; communication; and contingency planning.

Organizational Structure - The internal audit function should be positioned so the board has confidence that internal auditors will act impartially and not be unduly influenced by senior officers or operation managers. The audit committee should oversee the internal audit function, evaluate performance, and assign responsibility for the internal audit function to an internal audit manager or a member of management. If the responsibility is assigned to a member of management, the individual should not be involved in daily operations to avoid potential conflicts of interest. The internal audit manager should understand the internal audit function and have no responsibility for operating the system of internal control. Ideally, the internal audit manager should report directly and solely to the audit committee regarding audit issues and administrative matters such as resources, budget, appraisals, and compensation. If the internal audit manager is placed under a dual reporting structure (reports to a senior officer and the audit committee), the board should weigh the risk of diminished independence against the benefit of reduced administrative burden. Additionally, the audit committee should document its consideration of the risk and any mitigating controls the institution has in place to maintain audit independence.

Management, Staffing, and Audit Quality - The internal audit manager is responsible for control risk assessments, audit plans, audit programs, and audit reports. Control risk assessments document the internal auditor's understanding of significant business activities and associated risks. These assessments typically analyze the risks inherent in each significant business activity, mitigating control processes, and any residual risks to the institution. Internal audit plans should be based on the findings of the control risk assessments. The plans should include a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and the resource budget. Internal audit programs should describe audit objectives and list the procedures to be performed during each internal audit review. Audit reports should generally present 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. The role should not include business-line oversight of control activities, such as approving or implementing operating policies or procedures. The audit committee should ensure that any consulting type work performed (e.g., providing advice on mergers, acquisitions, new products, services, internal controls, etc.) by the internal auditor(s) does not interfere or conflict with the objectivity of monitoring the internal control system.

The internal audit function should be staffed and supervised by people with sufficient expertise to identify operational risks and assess the effectiveness of internal controls. Internal audit policies, procedures, and work programs should be commensurate with the size and complexity of the internal audit department and institution.

Scope - The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's balance sheet and off-balance sheet activities. At least annually, the audit committee should evaluate and approve internal audit's control risk assessment(s), the scope of audit plans, and how much the audit manager relies on the work of outside vendors. The audit committee should also periodically review internal audit's adherence to approved audit plans and should consider expanding internal audit work if significant issues arise or material changes occur in the institution's structure, activities, or risk exposures.

The audit committee and management are responsible for determining the extent of auditing required to effectively monitor the internal control system. The expense of having a full-time audit manager or auditing staff is likely justified at institutions with complex structures or high-risk operations. However, the cost of having a full-time audit manager or staff may be prohibitive for institutions with less complexity and risks. Nevertheless, institutions without an internal audit staff can maintain an objective internal audit function by implementing comprehensive, independent reviews of significant internal controls. To be effective, competent individuals should design review procedures, and the individuals directing or performing the reviews must not be responsible for managing or operating the controls under review. The person completing the control reviews should report findings directly to the audit committee. The audit committee should evaluate the findings and ensure senior management takes appropriate action to correct any identified deficiencies.

Communication - Directors and senior management should encourage open discussions and critical evaluations of identified control weaknesses and any proposed solutions. Internal auditors should immediately discuss internal control weaknesses or deficiencies with the appropriate level of management. Significant matters should be promptly reported directly to the board of directors or its audit committee with a copy of the written report provided to senior management. Moreover, the board or audit committee should provide internal auditors

the opportunity to discuss their findings without management being present, and institutions should establish procedures for employees to submit concerns (confidentially and anonymously) about questionable accounting, control, or auditing matters.

Contingency Planning - Whether using an in-house audit staff or an outsourced arrangement, the institution should have a contingency plan to mitigate any significant discontinuity in internal audit coverage, particularly for high-risk areas.

Outsourcing Internal Audits

Outsourcing arrangements involve contracts between an institution and a vendor that provides internal audit services. The arrangements may involve vendors providing limited or extensive audit assistance. Regardless of the level of outsourced services, an institution's directors are responsible for establishing and maintaining effective internal controls and internal audit programs.

Financial institutions should consider current and anticipated business risks when establishing each party's internal audit responsibilities. Institutions should have a written contract/engagement letter that clearly distinguishes its duties and those of the outsourcing vendor. Such contracts typically include provisions that:

- Define the expectations and responsibilities of both parties;
- Set the scope, frequency, and fees of a vendor's work;
- Describe the responsibilities for providing and receiving information and reports about the contract work status;
- Establish a process for changing contract terms, such as expanding audit work if issues are found;
- State that internal audit reports are the institution's property, designated employees will have reasonable and timely access to the vendor-prepared workpapers, and the institution will receive workpaper copies if needed;
- Specify the locations of internal audit reports and related workpapers;
- Specify the period vendors must maintain the workpapers;
- State that vendor audits are subject to regulatory review and examiners will be granted full and timely access to the internal audit reports and related workpapers;
- Prescribe a process for resolving disputes and for determining who incurs the cost of consequential damages arising from errors, omissions, and negligence;
- State that the 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
- State, as applicable, that the vendor will comply with independence guidance established by the American Institute of Certified Public Accountants (AICPA), U.S. Securities and Exchange Commission (SEC), Public Company Accounting Oversight Board (PCAOB), or regulatory agencies.

Management should exercise appropriate due diligence in selecting vendors and periodically review outsourcing arrangements and vendor performance thereafter.

Communication among the internal audit staff, the audit committee, and senior management should not diminish because the institution engages an outside vendor. All work should be well documented, and any identified control weaknesses should be promptly reported to the institution's manager of internal audit. Decisions not to report findings to directors or senior management should be the mutual decision of the internal audit manager and the outsourcing vendor. In deciding what issues should be brought to the board's attention, the concept of *materiality*, as the term is used in financial statement audits, is generally not a good indicator of which control weakness to report. For example, when evaluating an institution's compliance with laws and regulations, any exception may be important.

Accountant Independence

Accounting firms risk compromising their independence if they perform internal and external audit functions at the same financial institution. The Sarbanes-Oxley Act of 2002 prohibits accounting firms from performing external audits of a public company during the same period they provide internal audit services. Non-publicly traded institutions that engage a firm to perform internal and external audit work in the same period are encouraged to consider the risks associated with compromised independence versus potential cost savings.

External Audit

Financial institutions should design external audit programs to ensure financial statements are prepared in accordance with Generally Accepted Accounting Practices (GAAP) and to alert management of any significant deficiencies in internal controls over financial reporting.

Section 36 of the FDI Act, as implemented by Part 363 of the FDIC Rules and Regulations, establishes annual independent audit and reporting requirements for insured depository institutions with total assets of $500 million or

more. The 1999 Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations (1999 Policy Statement) includes audit and reporting guidance directed at banks and savings associations with less than $500 million in total assets.

Examiners that identify weaknesses in external auditing programs should include appropriate comments and recommendations in the ROE.

Audit Committees

All banks are strongly encouraged to establish an audit committee consisting entirely of outside directors. Although it may be difficult to establish a committee that includes only outside directors in a small closely held bank, all banks should be encouraged to include outside directors on their board and appoint them to the audit committee.

At least annually, the audit committee or board should analyze the extent of external auditing coverage needed by the bank. The board or audit committee should consider the size of the institution and the nature, scope, and complexity of its operations when evaluating external auditing needs. Institutions should also consider the benefits of:

- Financial statement audits,
- Internal control reviews,
- Additional auditing procedures for specific periods, and
- Additional auditing procedures for high-risk areas or special concerns.

Decisions regarding these considerations and the reasoning supporting the decisions should be recorded in committee or board minutes. If examiners determine risks are present that require additional external auditing, they should make specific recommendations to address the issues.

External Audits of Financial Statements

External audits help boards meet their fiduciary responsibilities and provide greater assurance that financial reports are accurate and complete. The audits can benefit management by providing insight into the effectiveness of accounting and operating policies, internal controls, internal auditing programs, and management information systems.

Each bank is strongly encouraged to adopt an external audit program that includes annual audits of its financial statements by an independent public accountant (unless its financial statements are included in the audit of the parent company's consolidated financial statements). A bank that does so would generally be considered to have satisfied the objectives of the 1999 Policy Statement.

External Audit Reports

Each state nonmember bank that undergoes external auditing work, regardless of the scope, should furnish a copy of any reports by the public accountant or other external auditor, including any management letters, to the appropriate FDIC regional office, promptly after receipt. A bank whose external auditing program combines state-mandated requirements, such as completion of annual directors' audits, with additional procedures may submit a copy of the auditors' report on its state-mandated procedures that is supplemented by a report on the additional procedures. In addition, the FDIC requests each bank to notify the appropriate regional office promptly when any public accountant or other external auditor is initially engaged to perform external audit procedures and when a change in its accountant or auditor occurs.

If a bank chooses an alternative external auditing program, rather than an annual audit of the financial statements, the report produced under the alternative program should include a description of the procedures performed. For example, if the auditor's report states *procedures agreed upon with management* have been performed, the bank should be asked to supply a copy of the engagement letter or other documents that outline the agreed-upon procedures so the FDIC can determine the adequacy of the scope of the external auditing program.

Audits at Institutions Under $500 Million

Regulatory 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. However, institutions of less than $500 million (at the beginning of their fiscal year) may be able to use alternative methods (some of which may be required by individual state statutes) that include:

- *Reporting by an Independent Public Accountant on an Institution's Internal Control Structure Over Financial Reporting* - This is an independent public accountant's examination and report on management's assertion of the effectiveness of the institution's internal control over financial reporting. For a smaller institution with less complex operations, this type of engagement is often less costly than a financial statement or balance sheet audit. It should include recommendations for improving internal controls, including suggestions for compensating controls, to mitigate risks due to staffing and resource limitations. Management's assertion and the accountant's

attestation should generally cover lending and investing as these activities usually present the most significant risks affecting an institution's financial reporting.

- *Balance Sheet Audit Performed by an Independent Public Accountant* - This audit involves an institution that engages an independent public accountant to examine and report only on the balance sheet. As with the financial statement audit, the balance sheet audit is performed in accordance with Generally Accepted Auditing Standards (GAAS). The cost of a balance sheet audit is often 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 for State Required Examinations* - Some state statutes require state-chartered depository institutions to have specific procedures performed annually by their directors or independent persons. Depending upon the engagement's scope, the cost of the agreed-upon procedures or a state required examination might 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. Findings or results are usually presented to the board or the audit committee so they may draw conclusions about the quality of financial reporting or sufficiency of internal control. When choosing this type of external auditing program, the board or audit committee is responsible for determining whether the procedures meet the external auditing needs of the institution, considering the institution's size and the nature, scope, and complexity of its business activities.

If the audit committee or board, at institutions with less than $500 million in total assets, determines not to engage an independent public accountant to conduct an annual audit of the financial statements, the reason(s) to use an acceptable alternative or to have no external auditing program should be documented in meeting minutes. Examiners should determine whether the alternative audit selected is appropriate, adequately covers all high-risk areas, and is performed by a qualified independent auditor. Any identified weaknesses in the external audit program should be commented on in the ROE.

If a bank with less than $500 million in total assets chooses not to have an external audit of financial statements by an independent public accountant, examiners should, at a minimum, strongly encourage the bank to engage an independent auditor to perform an external audit. If high-risk areas are evident, examiners should recommend that the auditor review the areas, and that any other deficiencies in the auditing program be corrected, to ensure there is adequate coverage of operational risk areas.

If a bank with less than $500 million in total assets has no external auditing program, examiners should review the board minutes to determine the board's rationale. Strong internal audit programs are fundamental to the safety and soundness of a bank, but are usually an insufficient reason for not implementing an external auditing program. One program should complement the other. Typically the external audit program tests and validates (or invalidates) the strength of internal controls and the internal audit program. In such situations, examiners should discuss the benefits of external auditing programs with the board and recommend the bank reconsider its decision.

Audits at Institutions of $500 Million or More

All depository institutions should implement adequate audit programs. Institutions with total assets of $500 million or more are required to have external audit programs that conform to the audit and reporting requirements of Part 363 of the FDIC Rules and Regulations.

Institutions covered by Part 363 must:

- Prepare annual financial statements,
- Produce annual reports detailing management's responsibilities and assessing management's compliance with laws and regulations, and
- Provide appropriate report signatures.

Annual financial statements must be prepared in accordance with GAAP and audited by an independent public accountant.

Annual reports must contain a statement of management's responsibilities for:

- Preparing financial statements,
- Maintaining adequate internal controls and procedures for financial reporting, and
- Complying with safety and soundness laws and regulations.

Management's assessment of their institution's compliance with laws and regulations must state a conclusion as to whether the institution complied with applicable laws and regulations, and disclose any instances of noncompliance.

Management reports at institutions with $1 billion or more in consolidated assets must also provide an assessment of the effectiveness of the institution's internal control system and include statements that:

- Identify the internal control framework used to evaluate the effectiveness of controls,
- Indicate controls were considered during the assessment,
- Express management's conclusion as to whether the institution's internal control over financial reporting is effective as of the end of the fiscal year, and
- Disclose any material weaknesses in internal controls that were not remediated prior to the fiscal year-end.

The signature requirements for management reports are related to the type of financial statements used to meet annual reporting requirements. For example:

- If financial statements and management reports are prepared at the institution level, the management report must be signed by the chief executive officer and the chief accounting officer or chief financial officer of the institution.
- If financial statements are prepared at the holding company level and the management report is prepared at the holding company level, the management report must be signed by the chief executive officer and the chief accounting officer or chief financial officer of the holding company.
- If financial statements are prepared at the holding company level and the management report is prepared at the institution level (or if parts of the management report are prepared at the holding company level and other parts at the institution level), the management report must be signed by the chief executive officer and the chief accounting officer or chief financial officer of both the holding company and the institution. Note: The management report must clearly indicate the level (institution or holding company) at which each of its components is being satisfied.

Public Accountant Responsibilities

The independent public accountant engaged by the institution is responsible for:

- Auditing and reporting on the institution's annual financial statements in accordance with GAAS or PCAOB standards; and
- Examining, attesting to, and reporting separately on the assertions of management concerning the institution's internal control structure and procedures for financial reporting on institutions with total assets of $1 billion or more.

Reporting Requirements

Part 363 requires insured depository institutions to submit the following reports and notifications to the FDIC, the appropriate federal banking agency, and the appropriate state bank supervisor.

- An annual report must be filed within 90 days after the fiscal year-end for public institutions and 120 days after the fiscal year-end for institutions that are not a public company or a subsidiary of a public company. When required, the annual report must contain audited annual financial statements, the independent public accountant's audit report, management's statements and assessments, and the independent public accountant's attestation concerning the institution's internal control structure and procedures for financial reporting.
- Within 15 days after receipt, the institution must submit any management letter; the audit report and any qualification to the audit report; and any other report, including attestation reports, from the independent public accountant.
- Within 15 days of occurrence, the institution must provide written notice of the engagement of an independent public accountant, the resignation or dismissal of a previously engaged accountant, and the reasons for such an event.
- A written notice of late filing should be filed on or before the filing deadline if an institution is unable to timely file all or any portion of its Part 363 reporting requirements. The late filing notice shall disclose the institution's inability to file on time and the reasons in reasonable detail. It shall also state the date by which the reports will be filed.

In addition, Part 363 requires certain filings from independent public accountants. Prior to commencing any services for an insured depository institution under Part 363, the independent public accountant must have received a peer review or be enrolled in a peer review program that meets acceptable guidelines. Also, accountants must notify the FDIC and the appropriate federal banking supervisor when it ceases to be the accountant for an insured depository institution.

Audit Committee

Each institution subject to Part 363 must establish an independent audit committee of its board of directors. The members of the committee must be outside directors who are independent of management. Their duties include overseeing the internal audit function, selecting the

accountant, and reviewing with management and the accountant the audit's scope and conclusions, and the various management assertions and accountant attestations. Part 363 establishes the following additional requirements for audit committees of insured depository institutions with total assets of more than $3 billion: two members of the audit committee must have banking or related financial management expertise; large customers of the institution are excluded from the audit committee; and the audit committee must have access to its own outside counsel.

Holding Company Subsidiaries

Subsidiary institutions of holding companies, regardless of size, may file the audited, consolidated financial statements of the holding company in lieu of separate audited financial statements covering only the institution. Subsidiary institutions with less than $5 billion in total assets may also elect to comply with the other requirements of Part 363 at the holding company level, provided the holding company performs services and functions comparable to those required of the institution. If the holding company performs comparable functions and services, the institution may elect to rely on the holding company's audit committee and may file a management report and accountant's attestations that have been prepared for the holding company. Subsidiary institutions with $5 billion or more in total assets may elect to comply with these other requirements of Part 363 at the holding company level only if the holding company performs services and functions comparable to those required of the institution, and the institution has a composite CAMELS rating of 1 or 2.

The institution's audit committee may be composed of the same persons as the holding company's audit committee only if such persons are outside directors of the holding company and the subsidiary and are independent of both organizations' management.

If the institution being examined is not the lead bank in the holding company, the examiner should confirm that the institution qualified for and invoked the holding company exemption. The examiner should also review the holding company reports to determine if any pertinent information about the institution was disclosed.

Mergers

Institutions subject to Part 363 that cease to exist at fiscal year-end have no responsibility under this rule. If a covered institution no longer exists as a separate entity because it merged into another institution after the fiscal year-end, but before the date its reports must be filed, institutions are not required to file a Part 363 Annual Report for the last fiscal year of its existence. An institution should consult with the Accounting and Securities Disclosure Section in Washington, DC, and its primary federal regulator if other than the FDIC, concerning the statements and reports that would be appropriate to submit under these circumstances.

Review of Compliance with Part 363

When reviewing the audit report, examiners should carefully assess any qualifications in the independent accountant's opinion and any unusual transactions. In reviewing management's report and the accountant's attestation, special attention should be given to any assessment that indicates less than reasonable assurance of effective internal controls over financial reporting, or less than material compliance with designated laws and regulations. Notices referencing a change in accountants should be reviewed for possible *opinion shopping* and any other issues that relate to safety and soundness issues.

The board's annual determination that all members of the audit committee are *independent of the management of the institution* should also be reviewed. For institutions exceeding $3 billion in total assets, the examiner should review board determinations and minutes documenting that at least two members of the audit committee have banking or related financial management expertise and that no member is a large customer of the institution. Appropriate recommendations should be made in the ROE if any determination is deemed unreasonable.

At the first examination of an institution subject to Part 363, examiners should fully discuss any apparent violations with management and the board. Based on their judgment of the situation, examiners should focus discussions on educating officers and directors and making appropriate recommendations about future compliance. The ROE should indicate the status of the institution's implementation efforts if not yet in full compliance with the rule.

Examiners should convey to the regional accountant any concerns regarding an accountant or an accounting firm's auditing, attestation, or accounting policies and procedures that may necessitate evaluating peer reviews. If the regional accountant considers a peer-review workpaper evaluation warranted, the regional accountant will confer with the Accounting and Securities Disclosure Section about conducting the review. This referral does not preclude the regional office from filing a complaint or recommending an enforcement action against the accountant. Peer-review workpaper evaluations are generally appropriate only in unusual or egregious circumstances; therefore, they should be relatively rare.

Examiners should not provide any written representations concerning Part 363 to institutions or their independent outside auditors. Examiners should refer institutions or auditors to regional accountants if they receive such requests.

←

OTHER EXTERNAL AUDIT ISSUES

Communication with External Auditors

The Interagency Policy Statement on Coordination and Communication Between External Auditors and Examiners (1992 Policy Statement), includes guidelines regarding meetings between external auditors and examiners.

The FDIC encourages communication between its examiners and external auditors with the permission of an institution's management. Permission is deemed to have been given once an institution notifies the FDIC of the accountant's name or the accounting firm that it engaged as external auditor (by letter or by submitting a copy of the auditor's report to an FDIC regional office). Permission continues until the institution notifies the FDIC that its relationship with the external auditor was terminated or another auditor was engaged.

The FDIC encourages external auditors to attend exit meetings and other significant discussions at which examiners and management discuss examination findings. In addition, auditors may request a meeting to discuss relevant supervisory matters with any of the regulatory agencies involved in the institution's supervision. An auditor who determines that communication with the FDIC is warranted concerning a recent examination should contact the appropriate regional office. A regional office staff member, examiner, or field supervisor may discuss pertinent examination findings with the external auditor. Regulatory agencies will usually ask management to be represented at the meeting. However, an external auditor may request a meeting without management representation.

Requests for meetings and information can also originate with regulatory agencies. Examiners may request meetings, including confidential meetings, with an institution's external auditor if questions arise concerning matters on which the external auditor is knowledgeable. FDIC personnel should determine if the external auditor discovered any problems relevant to the FDIC. Furthermore, FDIC personnel may request copies of workpapers relating to services performed by the external auditor. In some instances, an FDIC examiner, field supervisor, or regional office staff member may determine that attending the meeting at which the audit report is discussed between an institution's auditors and its management or board of directors (or an appropriate committee) would be useful. The institution should be advised and asked to present the request to the auditor.

The 1992 Policy Statement encourages open communication between examiners and auditors, and suggests institutions should provide its external auditors a copy of certain reports and supervisory documents including: reports of condition, examination reports, regulatory correspondence, and any formal or informal regulatory agreements or actions.

Similarly, AICPA guidance suggests auditors should communicate with examiners. The guidance indicates auditors should consider reviewing communication from examiners, and when appropriate make inquiries of examiners. The AICPA guidance also indicates auditors should be responsive to examiner's requests to attend meetings between auditors and bank management, and that management's refusal to allow auditors to review regulatory material or to communicate with examiners would ordinarily be an audit scope limitation sufficient to prevent the auditor from rendering an opinion.

Workpaper Review Procedures

Examiners, in consultation with the regional accountant, may review external audit workpapers relating to audits of financial institutions or their holding companies. Workpaper reviews may enhance examiners' ability to scope an examination by identifying areas where audit work was sufficient to allow a reduction in examination procedures and by identifying higher-risk areas where examination procedures should be expanded. A workpaper review may be especially useful if an institution has asset quality problems, complex investments, aggressive accounting practices, mortgage servicing activities, or large deferred tax assets.

Before undertaking any workpaper review, examiners should coordinate activities with the state bank supervisor and primary federal regulator (if other than the FDIC) of the institution, its holding company, and any other holding company subsidiaries. No set of workpapers should be reviewed more than once by the agencies.

Examiners should review the workpapers of the independent public accountant or other auditor performing the institution's external auditing program when an FDIC-supervised institution has undergone a financial statement or balance sheet audit, and:

- Significant concerns exist regarding matters that would fall within the scope of the work performed by the institution's external auditors, or
- The institution has been, or is expected to be, assigned a UFIRS composite rating of 4 or 5.

However, when considering how best to use examination resources, examiners should exercise reasonable judgment with respect to performing an external audit workpaper review for these institutions. For example, it would be appropriate to conduct an external audit workpaper review for FDIC-supervised institutions when significant matters exist and the review is reasonably expected to provide an examination benefit. If examiners determine that a benefit would not be derived from performing an external audit workpaper review for an FDIC-supervised institution, examiners must document, and include in the examination workpapers, the reasons for not conducting the review.

Requests by the regional director for access to a public accountant's workpapers should be in writing and specify the institution to be reviewed, indicate the accountant's related policies and procedures should be available for review, and request that a staff member of the public accounting firm knowledgeable about the institution be available to answer questions. Because workpapers are often voluminous, examiners are expected to view them where they are located. Since these workpapers are highly confidential, examiners are encouraged to take notes of needed information and should request copies of only those workpapers necessary for their records. Examiners should not request copies of all workpapers.

Complaints Against Accountants

An examiner encountering possible violations of professional standards by a CPA or licensed public accountant should, if practical (after consulting with the regional office), discuss the matter with the accountant in an attempt to resolve the concern. If the concern is not resolved, the examiner should send a memorandum to the regional director, with a copy to the regional accountant, summarizing the evidence of possible violations of professional standards and the inability to resolve the matter with the accountant. After conferring with the Accounting and Securities Disclosure Section, the regional office may determine it is appropriate to inform the accountant that a complaint to the AICPA and/or state board of accountancy may be considered. Where notification of apparent violation of professional standards appears appropriate, letters should be concurrently forwarded by the regional director to the state board of accountancy in the institution's home state, the Professional Ethics Division of the AICPA (in the case of certified public accountants), the subject accountant or firm, and the RMS Accounting and Securities Disclosure Section.

In addition to violations of professional standards, complaints should also include evidence of substandard auditing work or lack of independence.

Third-Party Audits at FDIC's Request

Examiners sometimes determine an institution is involved in unique activities or complex transactions that are outside management's expertise. For example, the institution may carry certain complex financial instruments or other unusual assets on its financial statements at values management cannot adequately support and the examiner cannot confirm. Additionally, the institution may have certain internal control problems that require the expertise of an independent consultant to resolve properly.

In these situations, after receiving appropriate approval, examiners may request an institution to contract with an independent public accountant or other professional to perform specific work to address the identified concern. Such an assignment would not be included in the normal scope of work performed in external auditing programs. This additional work, when performed by an independent public accountant, may be considered an engagement to perform *agreed-upon procedures*, to issue a *special report*, or *to report on the application of accounting principles* under applicable professional standards. These latter two engagements are performed by an independent public accountant under GAAS or PCAOB standards, while agreed-upon procedures are performed under Generally Accepted Standards for Attestation Engagements (GASAE). If another type of professional is contracted to perform services for an institution, the professional may be subject to a different set of professional standards. Nevertheless, the important elements for the examiner to consider when evaluating the adequacy of the institution's contract with the professional are similar in all cases.

When the FDIC requires an institution to contract an independent public accountant or other outside professional for specific work, the regional office should ask the institution to provide the FDIC with a copy of the contract before it is signed. The regional office should review the contract to determine if it sufficiently describes the work to be performed so that the outside professional can understand the FDIC's expectations and be responsive to any specific work requirements. The contract or engagement letter should, at a minimum, include:

- A description of the work to be performed;
- The responsibilities of the accountant or other professional;

- An identification of any specific financial statement elements, accounts, or items on which the work is to be performed; the party responsible for recording them in the financial statements; and the basis of accounting of the specific elements, accounts, or items on which the work is to be performed;
- A reference to any applicable professional standards covering the work, such as auditing, attestation, and appraisal standards;
- A description of:
  - Any specific procedures to be performed,
  - Any specific information sources to be used,
  - The qualifications of employees who perform the work,
  - The time frame for completing the work,
  - Any restrictions on the use of the reported findings, and
  - A provision for examiner access to workpapers. For example:

    The workpapers for this (specify type of engagement, e.g., agreed-upon procedures, special report) are the property of (name of firm) and constitute confidential information. However, (name of firm) agrees to make the workpapers supporting this engagement available to the FDIC and other federal and state banking regulators. In addition to the workpapers, (name of firm) agrees to make any or all of the following available to the FDIC and other federal and state banking regulators:

    - The work plan or similar planning document relating to this engagement;
    - The process used for the selection of samples used in the specific work, if applicable; and
    - Other pertinent information on the firm's policies and procedures that may affect this work plan.

    Access to the workpapers will be provided at (name of firm) local office under the supervision of our personnel. Furthermore, upon the request of the FDIC or other federal and state banking regulators, we agree to provide photocopies of selected workpapers to them.

←

SARBANES-OXLEY ACT

The Sarbanes Oxley Act of 2002 (SOX Act) was enacted to protect investors from fraudulent accounting activities by corporations. Protections center on annual financial disclosures and requirements that management and auditors establish internal controls and report on the adequacy of those controls.

The SOX Act is primarily directed toward companies that have a class of securities registered with the Securities and Exchange Commission or a federal banking agency. Applicability of the SOX Act to insured depository institutions depends primarily on an institution's size and whether it is a public company or a subsidiary of a public company.

Public Companies

Some FDIC supervised banks have securities registered pursuant to Part 335 of the FDIC Rules and Regulations and are therefore public companies. Other FDIC supervised banks are subsidiaries of public holding companies. Public companies and their independent public accountants must comply with the SOX Act, including provisions governing audit standards, management responsibilities, and financial disclosures.

Non-public Banks

Non-public banks generally do not fall within the scope of the SOX Act. However, existing regulatory guidance, such as Section 36 of the FDI Act and Part 363 of the FDIC Rules and Regulations, contains audit, internal control, and reporting requirements that mirror portions of the SOX Act. Although such practices are not mandatory for smaller, non-public institutions, the FDIC encourages all institutions to implement accounting, internal control, and reporting practices to the extent possible, given their size, complexity, and risk profile.

Reporting Requirements

Banks with total assets of $500 million or more at the beginning of their fiscal year are subject to the annual audit and reporting requirements of Section 36 of the FDI Act as implemented by Part 363 of the FDIC Rules and Regulations. Under certain circumstances, some institutions may satisfy Part 363 requirements by submitting audited, consolidated financial statements of their holding company. Key reporting requirements applicable to FDIC-supervised banks with $500 million or more in total assets include:

- Preparing annual financial statements in accordance with GAAP that are audited by an independent public accountant; and

- Preparing annual management reports that contain:
  - A statement of management's responsibilities for preparing financial statements, maintaining an adequate internal control structure, and complying with laws and regulations; and
  - An assessment by management of the institution's compliance with such laws and regulations during such fiscal year.

←

EVALUATING AUDIT PROGRAMS

Examiners should evaluate audit and control procedures as part of their overall assessment of a bank's internal control program. Each bank presents unique situations to which common sense and technical knowledge must be applied. Examiners should consider an institution's risk profile, size, complexity, number of employees, etc., when determining the overall adequacy of an internal control program.

Recommendation Considerations

Examiners should inform management and the board if they identify material or numerous internal routine and control deficiencies. When deficiencies are considered to be of sufficient importance, appropriate comments should be included in the ROE. Examiners should make recommendations for corrective actions only after considering the following:

- Recommendations should have merit. Criticisms that could be regarded as petty or highly technical may not help improve the bank's control environment.
- The benefit to the bank of implementing a recommendation should be emphasized.
- Recommendations or criticisms should be discussed fully with management prior to bringing it to the board's attention, as the record or procedure being criticized may be more fully understood by a banker who can offer a persuasive reason for its continuance.
- Examiners should not recommend banks maintain records in a specific format, or obtain software or accounting forms from a particular vendor.
- Convincing management to implement corrective actions is best accomplished by identifying material deficiencies and recommending effective solutions. Discussing minor deficiencies with management and making verbal recommendations (which should be documented in examination workpapers) may result in more effective correction of non-critical deficiencies.
- The relative importance of an individual control or lack thereof must be viewed in the context of other related controls.

Troubled Banks

Examiners should identify banks that have not had audits performed by an independent public accountant and at which any of the following conditions exist:

- Internal controls or internal auditing procedures are inadequate,
- The directorate is generally uninformed in the area of internal controls,
- There is evidence of insider abuse,
- There are known or suspected defalcations,
- There is known or suspected criminal activity,
- It is probable that director liability for losses exists,
- Direct verification is warranted, or
- Questionable transactions with affiliates have occurred.

In these situations, the examiner and regional office staff should consider adding a provision to any contemplated administrative order that the bank obtain an audit or, if more appropriate, have an independent public accountant or other qualified independent party perform specified audit procedures. Because each situation is unique, the examiner and regional office must evaluate the type of external audit program most suitable for each troubled bank and, in conjunction with regional counsel, ascertain that the inclusion of such an external audit program as a condition in an order is appropriate. Whenever a condition requiring an audit or specified audit procedures is included in an order, it should include requirements that the bank promptly submit copies of the auditor's reports to the regional office and notify the regional office in advance of any meeting between the bank and its auditors at which audit findings are to be presented.

Management Responsibilities

Assessing internal control programs is a critical part of examinations. In most cases, examiners can assess the adequacy of a bank's internal controls by reviewing:

- The overall structure of audit and control programs, monitoring procedures, and reporting mechanisms;
- Various audit reports in conjunction with the completion of standard examination procedures; and
- A limited number of specific controls or audit procedures.

Examiners should focus on identifying and correcting systemic weaknesses when evaluating internal control programs. Serious program weaknesses may exist if management fails to:

- Delineate clear lines of authority and responsibility,

- Standardize risk assessment procedures,
- Segregate operating and recording functions,
- Provide adequate and qualified audit personnel, or
- Regularly review and respond to audit reports.

In some instances, internal controls, monitoring procedures, reporting mechanisms, or financial conditions may indicate that more extensive audit tests should be undertaken. Testing procedures that may help identify errors, fraud, or insider abuse are discussed in the Examination Techniques section below. Examiners should refer to the Bank Fraud and Insider Abuse section of this Manual if they identify material errors or irregularities.

Common Controls

The following functions and related audit procedures should be included in most audit programs. The list is not all-inclusive and deficiencies in any one area may not represent an overall inadequate control program.

Cash and Due From Audits

The primary objectives of cash and due from audits are to ensure account balances are properly recorded, cash items clear within a reasonable period, and due-from accounts are substantiated and tested.

Auditors should periodically verify cash on hand, cash items, overdrafts, and other assets or liabilities held in suspense to ensure items are properly controlled, recorded, and disposed.

Due from reconciliations should be reviewed each month by someone who does not regularly reconcile the accounts. Particular emphasis should be placed on reviewing old or recurring items. Auditors should obtain account statements from depository institutions as of the audit date, and subsequent to the audit date, for validating bank reconcilements and ensuring outstanding items are cleared. Auditors should review all return items for an appropriate period after the audit date.

Investments

The primary objectives of investment audits are to ensure:

- Physical security certificates are on hand or held in safekeeping by others;
- Book entries are properly recorded;
- Interest and dividend income and security gains or losses are properly recorded;
- Securities are properly recorded as held-to-maturity, trading, or available-for-sale;
- Personnel follow segregation-of-duty and joint-custody directives, and
- Temporary declines in value are identified.

Auditors should:

- Prove subsidiary records to the general ledger,
- Verify securities on hand or held by others for safekeeping,
- Check the gain and loss entries on securities sold or matured since the previous audit,
- Review accrued interest accounts and substantiate computations and dispositions of interest income, and
- Assess premium-amortization and discount-accretion calculations.

Loans

Auditors should periodically:

- Prove subsidiary records to the general ledger,
- Verify a sampling of loan balances on a positive or negative basis,
- Verify the existence of negotiable collateral,
- Review accrued interest accounts and confirm the computation and disposition of interest income,
- Verify leases and related balance sheet accounts,
- Test unearned discount accounts, and
- Check rebate amounts for prepaid loans.

Allowance for Loan and Lease Losses (ALLL)

Auditors should:

- Review the balance of loans with charge-offs and the debit entries to the ALLL account,
- Review the balance of loans with recoveries and the credit entries in the ALLL account,
- Check supporting documentation for loans charged off, and
- Determine compliance with GAAP regarding the ALLL methodology used to estimate credit losses on individually and collectively evaluated loans.

Bank Premises and Equipment

Auditors should:

- Review entries and documentation relative to purchases and sales of premises and equipment since the previous audit;
- Verify computations of depreciation, amortization, and impairment;
- Check computations of gains or losses on property sold; and

- Trace sale proceeds.

Other Assets and Other Liabilities

Auditors should ascertain the appropriateness of other-asset and other-liability accounts by reviewing related policies, procedures, and internal controls and ensuring transactions are properly authorized, recorded, and balanced.

Deposits

Auditors should:

- Reconcile subsidiary records to general ledger accounts,
- Verify account balances on a test basis,
- Review closed accounts and determine if the accounts were properly closed,
- Review activity in dormant accounts and insider accounts,
- Review overdrafts,
- Check the computation of service charges and trace postings to appropriate income accounts,
- Review accrued interest accounts and check the computation of interest expenses,
- Verify the numerical sequence of pre-numbered certificates of deposit and official checks,
- Reconcile and determine the validity of outstanding official checks,
- Examine documentation supporting paid official checks, and
- Test certified checks to customers' collected funds.

Borrowed Funds

Auditors should:

- Confirm borrowings were authorized in accordance with internal policies,
- Verify balances of borrowed funds,
- Ensure collateral for borrowings is properly identified and disclosed,
- Verify changes in capital notes outstanding, and
- Review related accrued interest computations and interest expense balances.

Capital Accounts and Dividends

Auditors should account for all unissued stock certificates, review capital account changes since the previous audit, check computations for dividends paid or accrued, and review board minutes to determine the propriety of dividend payments and accruals.

Other Control Accounts

Auditors should test rental income for safe deposit boxes, examine and confirm safekeeping items, and reconcile consigned items on hand.

Income and Expenses

Auditors should test income and expenses by examining supporting documentation for authenticity and proper approval, and should test accruals by either re-computing amounts or examining documents supporting such accruals.

Direct Verification

Direct verification is an effective method of confirming the accuracy and validity of certain accounts, particularly loan and deposit accounts. Direct verification should be an important part of all internal and/or external audit programs, and may be employed as an internal control separate from regularly scheduled audits.

There are two primary types of direct verification, positive and negative. When the positive method is used, the customer is asked to confirm whether the balance, as shown, is correct. When the negative method is used, a reply is not requested unless an exception is noted.

The positive method has advantages from an audit standpoint as it provides considerable assurance the customer has carefully checked the confirmation form. The negative method is less costly and provides a measure of protection in those institutions having a strong program of internal control. The positive method is recommended for loan accounts. The positive method is preferred for deposit accounts, but because of high volume and cost factors, the negative method is often employed.

It is suggested that at a minimum, large deposit accounts, public fund accounts, dormant accounts, and accounts with unusual or high volumes of activity be positively verified. Additionally, overdue loans and charged-off loans should be confirmed through positive verification.

Direct verification may be conducted for all customers within a specific account type or through an appropriate sample. The necessity for a complete verification of loans or deposits is rare. A partial verification of representative accounts is usually satisfactory.

Direct verification may be performed by bank staff or contracted to a third party. To be effective, the verification procedure (including follow-ups) must be completely controlled by someone that does not have responsibility for the accounts or records being verified.

←
FRAUD AND INSIDER ABUSE

Introduction

Financial institutions are highly susceptible to fraud, embezzlements, and theft; and bank personnel at every level have opportunities to commit dishonest acts. Uncovering fraud is not the primary reason examinations are conducted; however, examiners must be able to recognize fraudulent or abusive actions.

The following items include higher-risk accounts and common methods for manipulating financial records.

Loans

Forged or fictitious notes; accommodation loans; loans to insider-related shell companies; embezzlement of principal and interest payments; failure to cancel paid notes; use of blank, signed notes; embezzlement of escrow and collection accounts; commissions and kickbacks on loans; fraudulent loans to cover cash items and overdrafts; and diverted recoveries of charged-off loans.

Loan Collateral

Loans secured by fraudulent collateral such as altered, stolen, or counterfeit securities; certificates of deposit issued by illegitimate offshore banks; and brokered loans and link-financing arrangements where underlying collateral is not properly pledged or is prematurely released.

Deposits

Unauthorized withdrawals from dormant accounts; fictitious charges to customer accounts; unauthorized overdrafts; payment of bank-personnel checks against customer accounts or fictitious accounts; manipulation of items used to reconcile deposit trial balances; unauthorized withdrawals from accounts where the employee is acting as an agent or in some other fiduciary capacity; withholding and destroying deposit tickets and checks; misappropriation of service charges; check kiting; and manipulation of certificates of deposit, money orders, and official checks.

Correspondent Bank Accounts

Concealing a shortage by unreasonably delaying the recording of cash letters; delayed remittance of cash letters; fictitious credits and debits; manipulations to prevent the detection of overstated balances, such as issuing drafts without corresponding recordation on the bank's books or credit to the account; overstatement of cash letters and return items; and false collection items.

Tellers and Cash

Lapping deposits (covering one day's shortage with the next day's receipts); theft of cash; excessive over and short activity; fraudulent checks drawn on customers' accounts; fictitious cash items; manipulation of cash items; and intentional failure to report large currency transactions or suspicious activity.

Income and Expense

Embezzlement of income; fraudulent rebates on loan interest; fictitious expense charges; overstated expenses; and misapplication of credit life insurance premiums.

Investment Securities

Collusion between a bank employee and a securities dealer to trade securities at inflated prices; concealing trading losses from bank management and examiners; and unauthorized purchases and sales of securities, futures, or forward contracts with benefits accruing to a bank employee. Improper securities trading practices include:

- Placing personal trades through bank accounts, thereby obtaining the advantage of the bank's volume discounts on commissions;
- Purchasing or selling an issue of securities prior to executing bank or trust account trades, which could be expected to change the price of the security thereby providing a personal price advantage (front-running);
- Purchasing and selling the same securities on the same day with the trader retaining the gains from any price increase, but assigning losses to trust accounts if prices decrease; and
- Buying or selling based on nonpublic, inside information, which might affect the price of securities thereby enabling the trader to benefit personally from the transaction.

Additional Risks

Numerous methods are used to defraud banks and pose an ongoing problem. While no bank is exempt from the threat of defalcations by management, employees, or outsiders, certain institutions are more vulnerable than others. Any of the following situations may indicate the need to use more comprehensive audit techniques:

- An institution has one officer with dominant control over a bank's operations.
- Audit programs are inadequate.

- Internal control deficiencies are evident, such as weak vacation policies or ineffective segregation of duties.
- Records are poorly maintained or carelessly handled.
- Close supervision by the board of directors or senior management is inadequate, especially where rapid growth has occurred or numerous inexperienced managers are employed.
- A bank has grown substantially in a short time period. (The growth may have involved the use of high deposit rates, brokered funds, fraudulent or poor quality loans, or dishonest acts to conceal the bank's true condition.)
- A bank has had limited growth or a steady decline in deposits despite general economic prosperity in their operating area or strong growth by competing institutions.
- Earnings and yields are below average and expenses are high in comparison with past operating periods with no apparent explanation for the change.
- The bank is experiencing abnormal fluctuations in individual revenue or expense accounts, either in terms of dollar amounts or in relation to other operating accounts.

←

EXAMINATION TECHNIQUES

Introduction

Numerous methods for concealing fraud exist, and even comprehensive audit techniques may not expose deceptive practices. However, when necessary, examiners should conduct detailed audit procedures. The audit techniques described below are not intended to be used at every examination; however, examiners should consider using these or similar techniques when appropriate.

Examiners should consult with the regional office if fraud-related examination procedures appear warranted.

Account Reconcilements

Examiner-prepared reconcilements of asset, liability, and capital accounts help ensure entries are properly recorded and subsidiary account records balance to the general ledger.

Direct Verification

Direct verifications are rarely initiated by regulatory personnel. Typically, financial institutions perform the verifications as part of their comprehensive audit function. If examiners, in consultation with regional office personnel, determine direct verifications are necessary, it is preferred that the bank or its external auditors make the customer contacts as these parties can more efficiently verify transactions with bank customers.

However, in certain situations it may be necessary for the FDIC or another banking agency to perform direct verifications. This may be appropriate if significant unreconciled items are disclosed, or evidence of potential fraud exists. Regional director approval must be obtained before examiners initiate direct verification of bank accounts or transactions. The following basic procedures or guidelines should be used if direct verifications are performed by FDIC staff.

- Addressing, stuffing, sealing, and mailing of envelopes should be done by examination personnel only.
- Franked envelopes furnished for reply should be preaddressed to the field office, regional office, or a post office box rented for the purpose.
- Duplicate records of all items verified should be maintained for control purposes.
- Examiners should watch for borrowers with common addresses or post office box numbers and for accounts having the same addresses as bank officers and employees.
- Loan verifications should include charged-off notes; separate notices should be sent to primary obligors, co-makers, endorsers, and guarantors.
- Third-party guarantees on lines of credit or individual notes should be verified directly with guarantors, not through primary obligors.
- Deposit verifications should be considered for recently closed dormant accounts, overdrawn accounts, and pledged accounts.
- All replies should be compared against retained duplicate records. Exceptions should be fully investigated against bank records or through follow-up correspondence with customers.
- Undelivered and returned tracers, unacknowledged verifications, and unexplained differences should be discussed with the entire board, not just with officers.

Loans

Examiners should consider using the techniques discussed below during loan reviews, especially if credit administration is weak or if they identify potential irregularities.

- Compare the signature on a note with other notes or documents signed by the maker.
- Review bank records to determine who actually pays the interest and principal (and the source of the funds) on large lines of continuous credit.

- Review records for power-of-attorney agreements giving an individual other than the named borrower(s) control of loan proceeds. (The agreements may be a sign of straw/nominee loans.)
- Review records for any changes to the official signers on deposit accounts established to receive loan proceeds. This may allow individuals other than the named borrower(s) to control loan proceeds.
- Investigate weak credit lines where directors or management may be the interested party although the bank's records do not reflect their interests.
- Spot check a cross section of out-of-territory loans to verify the disbursement of loan proceeds and the source of principal and interest payments.
- Audit the interest collected on a sampling of loans. Review the loan interest account for several days and compare the total with journal figures and the amount credited to the general ledger.
- Compare collateral records to loans secured by such collateral, and compare the collateral receipt date with the date the loan was granted.
- Review charge-offs in banks with large or numerous charge-offs. Verify the amount charged off was the approved amount; determine who prepares the list of charge-offs, who collects recoveries, and the accuracy of the reporting of these items. Compare actual loan documents with the bank's records to confirm balances and signatures.
- Consider tracing the proceeds of large loans and lines of credit that are subsequently charged off. (Tracing loan proceeds involves following the trail of funds from initial and subsequent loan disbursements to determine the person or entity that ultimately received the funds and how the funds were used. Disbursements may be transmitted by cash, check, wire transfer, other electronic means, or a credit to deposit/loan accounts at the bank.) When large loans are funded or material loan losses incurred, it may be advisable to analyze credits by tracing disbursement of loan proceeds and reviewing the borrower's deposit account(s) for possible payments of commissions or fees to a bank officer.
- Consider the following when reviewing the recordkeeping and monitoring of principal and interest receipts, especially payments relating to revolving accounts-receivable (A/R) financing:
  - Review records for occurrences of lapping payments. (Lapping occurs when an employee misappropriates funds (such as a loan payment), and covers the theft with payments from another loan customer or from advance (early) payments from the same customer.)
  - Review records for occurrences of payments made through the creation of fraudulent notes or unauthorized use of dealer reserve accounts.
  - Check records for an unusually large number of advance payments or overdue loans. In suspect cases, trace a sample of transfers to and from borrowers' checking accounts.
  - Spot check a cross-section of loans for appropriate signatures, disposition of proceeds, collateral, and sources of payment (particularly if outstanding loan volumes increased substantially between examinations for no apparent reason and overdue loans are unusually low or high).
  - Review records for occurrences of loan payments that come from the proceeds of other loans. Be watchful for multiple payments made on the same date for a particular note or borrower and compare the total of the payments with new loans granted on or about the same date.
  - Spot check for adequate recordkeeping if indirect dealer-paper lines are poorly monitored.

Deposits

Risks associated with inappropriate deposit account transfers are elevated in banks with weak internal controls and audit programs. Consider the following items when investigating potentially improper activities relating to deposit accounts.

- Reconcile subsidiary and general ledger accounts and any related adjustment items such as return items, overdrafts, holdovers, or service charges.
- Review any unusual or unapproved withdrawals from inactive or dormant accounts.
- Compare cash items, rejects, and exception items to individual account records to determine if the accounts exist, have sufficient funds, or have been closed.
- Cross check the interest paid on certificates of deposit to the interest expense account to verify ownership, dates, amounts due, and amounts actually paid.
- Be alert for possible check kiting when reviewing accounts. When available, review reports on kiting suspects and uncollected funds. Kiting characteristics include a high number of daily deposits, a high percentage of deposits coming from accounts under common control of a kiting suspect, large round-dollar checks, total daily debits and credits of similar amounts, and small average balances.
- With a bank employee, reconcile incoming cash letters and local clearings, and sight-post items to demand account records to determine if there is an account for each item. If the cash letter has already been opened, compare the number of items listed on the tape accompanying the letter with actual items to ascertain whether any items have been removed.

Correspondent Bank Accounts

The following audit steps can be used when evaluating correspondent accounts:

- Reconcile subsidiary and general ledger accounts, and compare a sample of paid and cancelled drafts drawn on correspondent banks to ledger entries for the same days. Select appropriate test periods, such as the date, and for several subsequent days after, material business activities occurred or the date institutions were notified of upcoming examinations.
- Review prior internal reconcilements of cash due from correspondents and statements received from correspondents. Ensure the reconcilements identify large outstanding items, unusual activity, forced balancing, and unreasonable or ongoing delays in crediting correspondents for their charges. (Delays in remitting for cash letters can be used to cover defalcations.) Also, ensure irregular items are properly reported.
- Review entries of similar amounts and dates between correspondent accounts that may indicate possible kiting or shortages between correspondent accounts.
- Compare coin and currency transactions reflected on correspondent accounts to the bank's increase or decrease in the cash account on corresponding days.

Tellers and Cash

When warranted, tellers' daily cash records can be inspected for possible discrepancies such as mathematical errors, forced balancing, unusual charges or adjustments, and excessive total balances or number of cash items. Items drawn on or by bank personnel should always be verified as to final payment or disposition. All work can be checked for proper endorsements and dates that indicate a teller is carrying items for an excessive period.

Suspense Accounts

Suspense accounts are sometimes used to conceal shortages, worthless assets, and deposit diversions. Review suspense accounts for material, stale, or unusual items, especially noting the recurring use and aging of reconciling items.

Income and Expense Accounts

Examiners can test interest computations on a sample of loans and securities. Verify large, recurring, or unusual debits to income accounts, and test interest rebates on loans and monthly service charges on demand deposits. Finally, compare interest paid on time and savings deposits to the amount credited to respective control accounts.

General Ledger Accounts

Determine the reason for any unusual activity in general ledger accounts, or abnormal variations between various general ledger accounts, and assess the validity of any reversing or correcting entries. Select appropriate test periods, such as the date, and for several subsequent days after, material business activities occurred or the date institutions were notified of upcoming examinations. Trace all closing income entries to the undivided profits account.

Other

Be alert for any major changes, particularly growth, in asset or liability totals. In cases of rapid loan expansion, check for possible out-of-territory loans to insiders. Also, if loans and certificates of deposit have increased beyond normal expectations, check the source of certificates of deposit; check for tie-ins between new notes and new certificates of deposit as to common names, amounts, and dates; trace the proceeds and determine the source of principal and interest payments on potentially inappropriate new loans.

Secretary of State Websites

Many states have websites examiners can use to obtain useful information on an entity's corporate structure, principal shareholders, or officers and directors. The websites may also contain information on the principals' other business relationships.

←

RELATED CONTROL ISSUES

Information Technology

Part 364 of the FDIC Rules and Regulations requires financial institutions to have internal controls and information systems commensurate with the size of their institution and the nature, scope, and risk of their activities. Appendix B of Part 364 requires banks to have information security programs that include administrative, technical, and physical safeguards. Program standards should be designed to:

- Ensure the security and confidentiality of customer information;
- Protect against anticipated threats to the security or integrity of such information;
- Protect against unauthorized access to, or use of, information that could result in substantial harm or inconvenience to any customer; and
- Ensure the proper disposal of consumer information.

A bank's board of directors, or an appropriate board committee, should:

- Approve a written information security program;
- Oversee the development, implementation, and maintenance of the program;
- Assign specific responsibility for implementing the program; and
- Review reports from management.

Information systems present a variety of risks that, if not adequately managed, can negatively affect the safety and soundness of the institution. Therefore, examiners should assess information technology controls and operations at every examination. If an institution's internal control systems do not meet the program standards described above, the deficiencies should be described in the ROE.

Institutions should maintain a comprehensive security plan in order to maintain the confidentiality, integrity, and reliability of information. The plan should include regular risk assessments and, at a minimum, address physical and logical security, and backup and contingency strategies.

Generally, IT risk assessments consist of the identification of hardware, software, and information; an analysis of internal and external threats to the assets; and an evaluation of existing controls. The findings can provide management valuable information regarding the security of IT assets and any controls that may need strengthening. Management should use the information to develop strategies for improving identified control weaknesses and mitigating identified risks.

The FFIEC IT Examination Handbook, which comprises a series of booklets, serves as a reference for managing and examining IT systems. The Handbook contains IT examination procedures, workprograms, and references to related laws, regulations, and examination policies. It also provides examiners with fundamental principles of internal controls applicable to information processing environments. The FFIEC procedures and workprograms are the primary tools for the examination of large, complex data centers in financial institutions and independent technology service providers.

Examiners can also use portions of the FFIEC procedures and workprograms when necessary to review complex or high-risk areas during IT reviews of less complex, well-managed institutions.

Management Information Systems

The term *management information system* (MIS) broadly refers to a comprehensive process, supported by computer-based systems, that provides the information necessary to manage an organization. An effective MIS is essential in all institutions, but becomes increasingly important for managing risks in larger institutions with diverse business lines or a wide geographic footprint. Essential components of an effective MIS include timeliness, accuracy, completeness, consistency, and relevance. Management decisions may be invalid if any one of these components is compromised.

To evaluate an MIS, and ultimately the foundation upon which management's decisions are based, examiners should scrutinize each of the essential components. First, information must be current and available in a useful format to all appropriate users. This necessitates the prompt collection and editing of data. Second, an effective system of internal controls must be in place to ensure information is accurate and complete. Third, strategies and decisions cannot be adequately monitored or measured unless the information provided is consistent. Variations in how data is collected or reported can distort its usefulness, particularly in trend analyses. Any change in information collection or reporting procedures should be clearly defined, documented, and communicated to all users. Finally, the information provided must be relevant to the user. Reports that are overly complex or include unnecessary information impede users' ability to make effective decisions. Conversely, reviewing information from numerous reports can hinder analysis; therefore, a key consideration in the adequacy of reports is that they present information in a comprehensive, yet concise format.

Payment Systems

Financial institutions process a variety of payment instruments using various clearing and settlement systems. The systems are generally differentiated as wholesale or retail systems.

Although there is no definitive division between retail and wholesale payments, retail payment systems generally involve transactions between two consumers or between consumers and businesses and have higher transaction volumes and lower average dollar values.

Key risks in payment and settlement systems include:

- Credit Risk - The possibility a counterparty will not settle an obligation for full value either when due, or anytime thereafter.
- Liquidity Risk - The possibility a counterparty will not settle an obligation for full value when due.
- Operational Risk - The possibility of loss resulting from external events or inadequate internal processes,

people, or systems. This type of risk includes physical and logical security threats.
- Legal Risk - The possibility of loss because of the unexpected application of a law or regulation, or because a contract cannot be enforced.

Risk profiles vary significantly based on the size and complexity of an institution's payment-system products and services, IT infrastructure, and dependence on third parties. All financial institutions should maintain an effective internal control environment commensurate with the level of payment products and services offered. Detailed procedures for reviewing retail and wholesale payment systems are covered in the FFIEC IT Examination Handbooks.

Lost and Stolen Securities Program

The SEC started the Lost and Stolen Securities Program in 1977 to reduce trafficking in lost, stolen, missing, and counterfeit security certificates. Security certificates are documents representing, or claiming to represent, ownership in a security.

A security may be certificated or uncertificated. Ownership of a certificated security is represented by a security certificate. Ownership of an uncertificated security is not represented by a physical document, but simply by registration on financial records (book entries). The vast majority of securities are held in book entry form with a custodian.

Banks may acquire certificated securities when investing, holding securities as trust assets or collateral for loans, or through transfer agent activities. In each situation, a bank might acquire a security certificate that was reported as lost, stolen, counterfeit, missing, or otherwise encumbered.

The SEC implemented Rule 17f-1 to govern the reporting and recordkeeping of securities as a means for reducing trafficking in lost, stolen, missing, and counterfeit securities. The Securities Information Center (SIC) operates the SEC's Lost and Stolen Securities Program. The SIC may be contacted at the Securities Information Center, Inc., P.O. Box 55151, Boston, MA 02205-5151 or at www.secic.com.

Registration

All registered FINRA[1] broker dealers, FDIC-insured banks, and transfer agents that handle physical certificates must be registered with the SIC in order to report securities to the SIC database, or make database inquiries. Banks that did not handle certificated securities within the last six months do not need to be registered.

Registration can be direct or indirect. Banks registered as direct inquirers are allowed to make inquiries against the SIC database. Banks registered as indirect inquirers must have an agreement with a direct inquirer who makes inquiries on their behalf. In either event, institutions may inquire of the SIC whether a certificate has been reported as lost, stolen, counterfeit, missing, or otherwise encumbered (restricted, cancelled, escheated, etc.).

Inquiries

Insured depository institutions are required to make inquiries by the end of the fifth business day after a securities certificate comes into their possession, provided that such inquiries shall be made before the certificate is sold, used as collateral, or sent to another reporting institution (which includes broker dealers, transfer agents, and clearing agencies). Inquiries are not required if the securities certificate:

- Was received directly from the issuer or issuing agent at the time it was issued;
- Was received from another reporting institution or Federal Reserve bank or branch;
- Was received from a bank customer and is registered in the name of the customer or its nominee, or was previously sold to the customer as verified by internal bank records;
- Was part of a transaction having an aggregate face value of $10,000 or less in the case of bonds, or an aggregate market value of $10,000 or less in the case of stocks; or
- Was received directly from a drop that is affiliated with a reporting institution for the purposes of receiving or delivering certificates on behalf of the reporting institution.

Reporting

Reporting requirements vary based upon the type of issue being reported and the type of entity doing the reporting. In general, banks should report:

- Stolen security certificates (or the loss of any securities where criminal activity is suspected), to the SIC and the registered transfer agent for the issue, within one business day of the discovery. If the certificate numbers of the securities cannot be determined within one business day, they should be reported as soon as possible. Stolen securities must also be promptly reported to the Federal Bureau of Investigation.

1 The Financial Industry Regulatory Authority (FINRA) is an independent regulator for securities firms doing business in the U.S.

- Security certificates missing or lost for a period of two business days, to the SIC and the registered transfer agent, within one business day of the discovery. Certificates lost, missing, or stolen while in transit shall be reported by the delivering institution.
- Counterfeit securities to the SIC, transfer agent, and Federal Bureau of Investigation within one business day of the discovery.
- Otherwise impaired security certificates on a voluntary basis. The SEC encourages institutions to report on and inquire about encumbered certificates that are not specifically subject to Rule 17f-1, such as restricted, cancelled, or escheated certificates.

Banks that recover a lost, missing, or stolen securities certificate must report recoveries to the SIC and registered transfer agents within one business day of recovery. The recovery of certificates that were reported lost, missing or stolen and involved allegations of criminality must also be reported to the Federal Bureau of Investigation.

Banks must report lost, stolen, or counterfeit items on SEC Form X-17F-1A. Reports to the Federal Bureau of Investigation may be made on SEC Form X-17F-1A or Suspicious Activity Reports.

Note: Institutions must file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network within 30 days of discovery for:

- Insider abuse involving any amount,
- Transactions aggregating $5,000 or more where a suspect can be identified, or
- Transactions aggregating $25,000 or more regardless of potential suspects.

Refer to 17 CFR Part 240, Rule 17f-1 for a complete description of all reporting requirements.

Exemptions

The following types of securities are not subject to the SEC's inquiry and reporting requirements:

- Security issues not assigned CUSIP numbers,
- Bond coupons,
- Uncertificated securities,
- Global securities issues, and
- Any securities issue for which a negotiable securities certificate cannot be obtained.

Examination Considerations

Examiners should periodically:

- Ensure banks are directly or indirectly registered, or exempt from SEC registration requirements;
- Discuss Rule 17f-1 with bank personnel to evaluate their understanding of the rule;
- Review documentation relating to inquiries and reporting to ensure compliance with the rule; and
- Assess the adequacy of audit procedures covering the lost and stolen securities program.

Examiners should cite noncompliance with SEC Rule 240.17f-1 as an apparent violation on the Violations of Laws and Regulations page.

Improper and Illegal Payments

The Foreign Corrupt Practices Act (FCPA) and the Federal Election Campaign Act (FECA) cover improper and illegal payments by banks and bank holding companies. The FCPA prohibits bribes to foreign government officials to obtain or keep business.

The FECA prohibits national banks from making contributions relating to elections to any political office, including local, state, and federal offices. State-chartered institutions are also prohibited from contributing to any federal office, but may make contributions connected to state and local elections if authorized under their state's laws. However, all contributions must be properly authorized and recorded.

Improper methods for making political contributions may involve falsified expense accounts, below-market rate loans, providing equipment or services without charge, and paying bonuses to employees or excessive fees and salaries to officers that are then contributed to a campaign. These methods involve unacceptable accounting practices, and, if identified, reflect unfavorably on management and internal control and audit programs.

Examiners should consider the following items when evaluating the effectiveness of an institution's controls over political contributions.

1. Determine whether the bank has a policy prohibiting improper or illegal payments, bribes, kickbacks, loans, etc., relating to domestic and foreign governments or political campaigns.

2. If the bank has such a policy, review and analyze it for adequacy, and determine if it is appropriately communicated to officers, employees, and agents of the bank.

3. Review any audits or reports that evaluate policies or operations relating to funds or services provided in

connection with political campaigns. In addition, review any investigative reports generated by other government agencies.

4. Review and analyze any internal or external audit programs relating to political contributions and determine if the programs include appropriate procedures for discovering and reporting improper practices or illegal payments. Determine whether the programs remind auditors to be alert to any unusual entries or charges that might involve improper or illegal payments, and review the results of any related audits.

5. Analyze the general adequacy of internal controls to determine whether there is sufficient protection against improper or illegal payments under the aforementioned statutes.

6. If examination analysis indicates political-contribution audit programs or internal controls are inadequate, examiners should consider performing additional analysis, such as:

   - Reviewing income and expense account entries (and supporting documentation) since the last examination for large or unusual items.
   - Reviewing bank-controlled accounts, such as dealer reserves and cash/collateral accounts, to determine the validity of entries and adequacy of customer notifications. With respect to official bank checks, review copies of the checks and supporting documentation for unusual items or checks to political organizations or related individuals.
   - Reviewing charged-off loan files to determine the appropriateness of any charge-offs to government officials, or political candidates or political organizations.
   - Review new loan and time deposit relationships with public entities and municipalities that originated since the prior examination. Inquire about the nature and source of the new relationship(s). If inquiries raise suspicions, review credit underwriting documents and trace loan proceeds to resolve outstanding questions or concerns. Similar procedures should be conducted for customers identified as Politically Exposed Persons.

7. When performing routine examination procedures, examiners should be alert for any transactions, or the use of any bank services or equipment, that might involve bribes, political campaigns, or inappropriate political activities. The activities may be identified through the review of items such as:

   - Loans or lines of credit;
   - Income and expense entries;
   - Director, officer, and employee deposit accounts or overdrafts; and
   - Official checks and escrow accounts.

References:

- FFIEC IT Examination Handbooks
- Manual Section 9.1, Bank Fraud and Insider Abuse