




## Oversight by the Board of Directors

The board of directors oversees management activities and is ultimately responsible for the affairs of a savings association. Laws and regulations governing board activities require directors to exercise care and loyalty toward the savings association and not to advance their own personal or business interests at the expense of the savings association.

### RESPONSIBILITIES OF THE BOARD OF DIRECTORS

As the financial services industry continues to evolve, the duties of directors are becoming more complex and demanding. In addition, the corporate scandals of 2002 and the Sarbanes-Oxley Act have raised public awareness in the area of corporate governance. Today's board of directors must take an active role in shaping and controlling a savings association's business operations and risks. The following are some basic responsibilities the board has in actively overseeing the association's affairs:

LINKS	
	<a href="#">Program</a>
	<a href="#">Questionnaire</a>
	<a href="#">Appendix A</a>

- Establish business goals, standards, policies and procedures, and operating strategies and understand the risks involved in following certain strategies.
- Approve standards for ensuring that the savings association's transactions with affiliates are sound, and are considered solely from the association's interests.
- Establish a compliance program emphasizing the importance of regulatory compliance as an inherent part of business operations ensuring compliance with external standards, such as laws and regulations, and the association's own policies and procedures.
- Hire and retain executive officers with the skills, integrity, knowledge, and experience appropriate for the nature and scope of their responsibilities and periodically evaluate management's performance.
- Establish and maintain appropriate committees that have written charters delineating the committee's functions, responsibilities, and membership qualifications.
- Ensure that the association maintains a corporate existence that is separate from its affiliates, subsidiaries, holding company, and sister banks.

- Ensure that the association serves the credit needs of its community or communities and meets responsibilities under the Community Reinvestment Act (CRA).
- Review operating results, compliance performance and performance of new and existing activities.

In fulfilling these responsibilities, the board of directors should observe the following standards:

- Operate independently from management.
- Stay well informed and be attentive to risk.
- Attend board meetings regularly.
- Conduct business affairs ethically; avoid conflicts of interest and self-serving practices.

OTS federal charters for mutual and stock associations authorize the number of directors to be not fewer than five nor more than 15, except when the Director of OTS approves a lesser or greater number. A quorum for board meetings is the majority number of directors that an association's bylaws prescribe, even if the association has not yet elected the prescribed number.

For a list of board of directors' statutory and regulatory responsibilities, see the References at the end of this Handbook Section and the [Questionnaire](#).

### Analyzing Board Performance

Evaluating the effectiveness of a board of directors is an important examination function. The results often provide a useful indicator of an association's future condition and help OTS design a regulatory profile. In carrying out the evaluation, you should perform the following steps:

Evaluating the effectiveness of a board of directors is an important examination function.

- Tailor the scope of the examination to the risk profile of the association. A comprehensive assessment of each director and officer usually is not necessary.
- Concentrate on issues rather than on personalities. Analyzing the board's performance is a sensitive process that requires focusing on problem solving, not fault finding.
- Determine the level of director awareness and accountability. Board members should know and fulfill their responsibilities.

To evaluate board effectiveness you must review board minutes and other documents, interview management, and check on the board's response to supervisory directives. In rare instances, you may need to expand the scope of the examination and interview individual directors. You should only need

to do this if the information is unavailable from other sources. Meetings with the entire board provide an additional means of evaluating a board's effectiveness. See [Examination Handbook Section 070](#).

Directors generally welcome regulatory review and specific recommendations for improvements. In unusual cases, however, directors may be uncooperative or attempt to hide instances of incompetence, lack of care, or even fraud or criminal malfeasance. Possible causes for the condition of a troubled association include any of the following reasons:

- Self-dealings or other conflicts of interest.
- Unsafe and unsound practices.
- Management incompetence.
- Lack of director participation.
- Domination of the board by one director or officer.
- Disregard for the regulatory process.
- Lack of independence.

The board is ultimately responsible for prevention or correction of these problems. If the board is unable or unwilling to correct serious problems, you must act immediately to protect the association and ensure its safety and soundness. For more information in this regard, refer to [Examination Handbook Section 370, Enforcement Actions](#).

### *Board Minutes*

The primary sources of information you need to evaluate a board of directors and its actions are the minutes of its regular and committee meetings. You should review these minutes to determine the status of the following areas:

- Adequacy of management's reports to the Board – Management reports submitted to the board should be thorough and accurate and cover all aspects of the association's operations. Management should provide such reports to the directors before regular board or committee meetings to allow adequate time for review before the meetings.
  - Reports should document any significant changes to capital, financial performance results, compliance performance, and major business activities, including information technology risks.
  - Reports for technology risks should address information security, technology audit work, business continuity planning, and vendor oversight activities. Additionally, the minutes

should document that the board received a status report on and approved the association’s compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which implement Section 501(b) of the Gramm-Leach-Bliley Act of 1999.

- Oversight of management – Minutes should reflect the board’s discussion and approval of any major strategic or operating decisions and the adoption of major operating policies and procedures. Management should obtain board approval before implementing new policies or engaging in new activities.
- Attendance and participation – The minutes should evidence “regular” attendance by board members. Attendance at 75 percent of all regularly scheduled board meetings is the benchmark for “regular” attendance. Minutes should also identify board members who ask questions or make motions, indicating that they are active in the meetings. Another indicator of active involvement is participation on committees.
- Performance evaluations – Minutes should reflect the board’s election of officers, its review of management performance, and its deliberations regarding salaries and compensation for officers and fees for attorneys, appraisers, directors and others.
- Compliance with board directives – Savings associations should have internal systems to monitor operations and ensure that management’s actions are appropriate and conform to board-approved policies and directives.

Board minutes should be a complete and accurate representation of meeting discussions, including dissenting opinions or votes. Minutes should indicate that the directors studied pertinent documentation and based their decisions upon such documentation. Each director should have the opportunity to review and, if appropriate, modify the minutes before the board ratifies them. However, board minutes should never be altered to distort facts.

### *Reports to the Board*

A board’s excessive reliance on benchmark financial statistics rather than on comprehensive financial analysis suggests that the directors may not be overseeing the association’s affairs appropriately. Undue reliance on only a few indicators may result in erroneous evaluations of the association’s condition.

The quality of report information that management provides to board and committee members is critical in a board’s decision-making process.

Therefore, you should determine that the reports to the directors include information that is complete, supported, understandable, and accurate.

The quality of report information that management provides to board and committee members is critical in a board’s decision-making process. Not only must directors carefully review information that management provides,

they must also ensure themselves that the information is complete and contains all pertinent data required to oversee the association.

Each regular board meeting should include a review of financial reports. Directors should not accept questionable report figures at face value, but should question the information and verify it when necessary. The association should promptly follow federal or state examination report recommendations. The audit committee composed solely of outside directors, if necessary, should provide for annual audits by an independent accounting firm, and should ensure the establishment of and adherence to a system of internal controls.

#### Audit Committee

The board should appoint an audit committee composed of directors who are independent of management and free from any relationship that would interfere with the exercise of independent judgment as a committee member. Members should also be independent of operating personnel who audit procedures, systems, or records. Operating personnel may, however, attend meetings to provide necessary information.

The major responsibilities of the audit committee include:

- Handling relations with the independent auditor (such as to select the auditor and to discuss the scope and results of the audit).
- Improving internal auditing functions and controls.
- Establishing policies and procedures that ensure full and accurate disclosure of the association's financial condition.
- Monitoring management and staff compliance with board policies, laws, and regulations.
- Measuring the effectiveness of the association's compliance management program.

All insured institutions with total assets of \$500 million or more must have an independent audit yearly. If any savings association is a subsidiary of a holding company, it can satisfy this requirement by an independent audit of the holding company. See [Examination Handbook Section 350, Independent Audit](#). In addition, if a savings association is publicly traded, regardless of size, it is subject to the auditor independence and certain other internal control report requirements of Sarbanes-Oxley. See attached Appendix A, Applicability of Selected Sarbanes-Oxley Act Requirements to Financial Institutions. Ideally, independent auditors provide an objective look at the performance of the association. You should carefully review independent audits for the following red flags:

- A qualified or adverse opinion.
- Significant adjustments to net income or capital.
- Internal control deficiencies, especially if recurring or not reported by the internal audit.

- Significant variances in time spent by auditors on the premises or in the audit expense incurred by the institution.
- Significant disagreements between management and the independent auditors.
- Significant variances from findings in the reports of examination.
- Failure of management to submit a plan for the correction of deficiencies.
- Late audit reports (more than 90 days from fiscal year-end).

#### Compliance Officer and Audit

A compliance officer who has direct access to the board and all areas of operations plays a key role in the internal audit function. It is the responsibility of this officer to monitor the association's business transactions to ensure compliance with regulatory provisions and safety and soundness standards.

The compliance officer, the audit committee, or the outside auditor, should annually prepare a compliance audit report. An audit of this nature will give the association an opportunity to resolve any internal problems that might otherwise be the subject of an adverse examination report.

#### Qualified Management

A board's most important responsibility is to select a capable managing officer (or chief executive officer) for the association. The board is also responsible for appointing or approving other senior management. Although economic conditions are a major influence on a savings association's well being, capable management and personnel are the dominant factors that contribute to an association's success.

Directors should give the chief executive the latitude he or she needs to run day-to-day operations; therefore, the board must be certain that the person is competent and trustworthy. As a further control, the board should define a managing officer's duties and responsibilities in writing and establish an adequate management succession plan. (See [Examination Handbook Section 330, Management Assessment](#).) The board should also establish reasonable compensation packages, including appropriate incentives, for executive officers. In addition, the directorate is responsible for evaluating the performance of top management.

#### *Board Oversight of Management*

The board of directors must ensure that a savings association's management has procedures in place to implement board-adopted policies. The board should ensure that management performs the following functions:

- Hires and retains employees and agents with the skills, integrity, knowledge, and experience appropriate to the nature and scope of their responsibilities. Proactively engages and supervises vendors.
- Provides ongoing comprehensive training programs, including the association's information security program.
- Follows the board's direction and provides periodic reports to the board concerning policy compliance, such as interest rate risk exposure reports, earnings and capital projections and analysis, and information security.
- Develops, implements, and monitors a comprehensive compliance management program predicated on systems, real-time monitoring, periodic self-assessment, organizational accountability, responsiveness to needed improvements, and effective training (OTS's SMAART compliance program components).
- Maintains an awareness of regulatory issues and developments.
- Reviews the board's policies periodically and suggests changes when appropriate.
- Develops, tests, and implements a comprehensive, association-wide business continuity plan that reflects the technology environment.
- Implements and manages operations to achieve the board's financial objectives and establishes operational policies for financial functions.
- Supervises investment portfolio management activities. Invests excess liquid funds in securities that complement the association's overall risk/return profile.
- Maintains an awareness of the economic and interest-rate environment, particularly local economic conditions, prepayment trends, volatility, and related regulatory developments.
- Reviews asset quality, including trends in delinquencies, nonaccrual loans, real estate owned, and charge-offs and recoveries. Also reviews the adequacy of reserves and quantifies the effect of nonperforming assets on the risk/return profile.
- Develops, reviews, and monitors capital plans, business plans, information technology plans, and strategic plans. Integrates this role with the budgeting function. Also generates variance and rate and volume analysis reports.
- Provides adequate support, planning, and oversight when the association enters nontraditional banking activities, new business lines, or acquires and implements significant new technology. Considers these activities, which may be organizationally distinct from the association's

operations, in connection with the association's overall risk/return profile. Sets specific standards concerning risks and assumptions.

- Manages capital market activities, including capital raising, debt issuance, dividend policies, and merger and acquisition analysis. Considers these activities with the management of the association's overall risk/return profile.
- Ensures that product development activity and pricing comport with the association's overall risk/return objectives. Compares the savings association's product pricing to a sample of key competitors.

### Use of Consultants

Savings associations sometimes hire third parties, such as consulting firms, investment bankers, lawyers, accountants, or other professionals, to provide services not usually required in the normal course of business. Consultants normally provide such services before and during proposed mergers, systems conversions, implementation of new technology, capital raising efforts, major asset sales, boards of director's internal investigations, and defenses against regulatory determinations. The board of directors must justify and approve contracts that the association enters into with third parties. Using a third party to perform services does not diminish the board's responsibility to ensure that services are provided in a safe and sound manner, and in compliance with applicable laws and regulations. Generally, the risk management policies that apply to a savings association conducting an activity directly, also apply to third parties conducting activities on the association's behalf. See TB 82a, Third Party Arrangements.

The board of directors should remind management to take care in contracting with outside parties that propose to provide business plans or financial models at no direct cost to the association. Such vendors usually expect the association to transact business with them on an exclusive basis, and management may feel an obligation to do so. These vendors will have exclusive access to detailed information about the association that could lead to proposals or transactions that are not in the association's best interest.

The board should ensure that management does not rely on outside consultants to excess, or use overly simplistic assumptions.

The board should ensure that management does not rely on outside consultants to excess, or use overly simplistic assumptions.

### Policies and Procedures

The board establishes policies as guidelines for an association's activities. Procedures represent the methodology for implementing an activity. Operating policies and procedures are necessary to establish management's strategy to communicate the association's goals and to provide a basis for gauging performance.



The directors must provide a clear framework so that the managing officer can operate and administer the association's affairs. These areas include the business strategy as set forth in the business plan, investment and loan policies, capital planning, funds management, risk management, including technology risks and controls, information security policies and procedures, and compliance policies and procedures. The Handbook covers these areas in other sections. The board of directors must approve all major policies.

Board policies and procedures should meet the following parameters:

- Establish and provide guidance and direction for an association's operations.
- Exist for all major phases of the association's operations.
- Be tailored to the association's operations and risk profile.
- Provide guidance and promote controlled and efficient operating practices.

Management's implementation of board policies and procedures and the association's adherence to operating standards indicate the effectiveness of the board. Positive indications of successful implementation of policies and procedures include:

- Current policies and procedures.
- Established systems to support stated objectives.
- Required evaluations and benchmarks for measuring and monitoring performance.

### *Business Plan*

Directors are responsible for establishing a business plan that documents major financial policies, including funds management, lending, investments, dividends, growth, and interest rate risk management. For more information on the latter, refer to the Interest Rate Risk Management Handbook Section and Thrift Bulletin 13a. While management may develop such policies at the direction of the board, the directors must thoroughly review and give final approval to each contemplated policy. Directors must also approve the association's budget and ensure that it is realistic, allows for secure transactions, and reflects adequate capital.

Ideally, the board should have access to information on economic issues because the performance of the economy affects the savings association's performance. Early recognition of changes in the economy provides notice of new opportunities or potential deterioration of asset quality.

### *Setting Financial Goals: The Risk vs. Return Tradeoff*

Savings associations generally express overall financial return objectives in terms of net earnings maximization or net equity value maximization. These financial goals are subject to internal and

external risk factors. The greater the risk embedded in individual assets, portfolios, or the overall institution, the greater the variability of returns over time.

The board of directors and management must realize that the savings association can generate higher returns (earnings or equity value) only if the association takes on greater risk; this is the risk/return tradeoff. The choice between these two alternatives relates to the management of all the association's financial functions.

To manage risk effectively, a savings association must have an informed board of directors that is capable of guiding the association's risk strategy. It is important for the board to develop a rational decision-making process for determining a savings association's optimal risk/return profile. An analysis of the effect of numerous risk/return tradeoffs is crucial to successful financial management. See Examination Handbook Section 510.

#### Types and Sources of Risk Exposure

There are several significant types and sources of risk exposure applicable to savings associations. For each type and source, the board of directors must provide direction to management as to the extent of risk the association may undertake.

**Credit Risk** – The risk that the borrower or issuer will not repay principal or interest on loans or investments. This area of risk includes counterparty credit risk, which is the risk that the counterparties will not honor their commitments for items such as over-the-counter option transactions or derivative instruments.

**Interest Rate Risk** – The vulnerability of an association's financial condition to movements in interest rates. Interest rate risk arises from four sources: repricing (mismatched) risk, yield curve risk, basis risk, and options risk. Repricing risk, the primary source of interest rate risk, comes from timing differences in the maturity and repricing of assets, liabilities, and off-balance sheet positions. Yield curve risk arises when unexpected shifts of the yield curve affect a savings association's income or economic value. Basis risk arises from the imperfect correlation in the adjustment of the rates earned and paid on different financial instruments with otherwise similar pricing characteristics. Options risk arises from options, embedded in many financial instruments, that provide the holder with the right, but not the obligation, to buy, sell, or in some manner alter the cash flows of the instrument. See Thrift Bulletin 13a for a more detailed discussion of interest rate risk. TB 13a requires the board of directors to establish and maintain an association's interest rate limits.

**Liquidity Risk** – The risk that funds may not be available to meet cash outflows when they arise. Liquidity risk occurs when an association is unable to liquidate assets or obtain adequate funding to continue operating. This situation may occur if the association cannot easily unwind or offset specific exposures without significantly lowering market prices because of inadequate market depth or market disruptions.

**Compliance Risk** – The risk to earnings, capital and market viability as well as on investor, customer, and regulatory relationships arising from violations of or noncompliance with laws, rules, regulations,

industry practices, internal policies and procedures, ethical standards, or customer service goals. It exposes an association to fines, civil money penalties, litigation costs, diminished reputation, reduced franchise value, and reduced business opportunities.

Other Risks – Includes operational risk, legal risk, reputation risk, fraud and insider abuse risk, and disasters or catastrophe risks.

### Documentation

An integral part of a savings association's books and records includes documentation of all business transactions. The records should reflect regulatory compliance and adherence to safe and sound procedures. The directors should have full access to such records and use them in approving loans and other investment transactions.

To facilitate examinations each savings association, affiliate, and subordinate organization should establish and maintain accounting and other records that provide an accurate and complete record of all business it transacts. Associations, affiliates, and subordinate organizations must also ensure that the documents, files, and other material or property comprising the records shall always be available for examinations. For supervisory purposes, associations should retain these original business transaction records until the savings association has two regular examinations and the association and OTS resolve any supervisory matters raised in the examinations. Savings associations must also comply with the records retention requirements of safety and soundness, enforcement, compliance, nondiscrimination and consumer affairs laws and regulations.

Due to differing local customs and state laws, associations should obtain recordkeeping (including microfilming, microfiche, and digital imaging) guidance and advice from local sources, such as attorneys, independent auditors, and income tax consultants. OTS encourages associations to develop and follow a formal written recordkeeping policy and records retention schedule.

## Employment Contracts and Executive Compensation

This section provides guidance for review of compensation provisions and clarifies OTS policy on unsafe and unsound practices relating to executive compensation and employment contracts.

### *Definitions*

Compensation includes any payment of money or other items of value in consideration of employment. Compensation includes the following items:

- Base salary
- Commissions
- Bonuses

- Pension and profit sharing plans
- Severance payments
- Retirement
- Director or committee fees
- Fringe benefits
- Payment of expense items for a nonbusiness purpose, or that do not meet the IRS requirements for deductibility by the association.

OTS does not ordinarily consider the grant or exercise of stock options as compensation unless they are sufficiently material in amount or conditioned upon factors that result in incentives that cause supervisory concerns.

A senior executive officer includes any individual who holds the title or performs the function of one or more of the following positions (without regard to title, salary, or compensation):

- President
- Chief executive officer
- Chief operating officer
- Chief financial officer
- Chief lending officer
- Chief investment officer
- Chief compliance officer

Senior executive officer also includes any other person identified by OTS in writing as an individual who exercises significant influence over, or participates in, major policymaking decisions, whether or not hired as an employee.

An employment contract is any agreement, intended to be legally enforceable, that materially affects the terms and conditions of a person's employment.

A savings association is in troubled condition if it meets any of the conditions below:

- OTS notifies the association in writing that OTS has assigned the association a composite numerical rating of 4 or 5 under the Uniform Financial Institutions Rating System or an equivalent rating under a comparable OTS rating system.
- The association is subject to a capital directive, a cease and desist order, a consent order, a formal written agreement, or a prompt corrective action directive relating to the safety and soundness or financial viability of the association.
- OTS informs the institution, in writing, of its troubled condition based on information available to OTS. Such information might include current financial statements, reports of examination, or limited scope review of the institution.

### *General Policy*

OTS regulation 12 CFR § 563.39, Employment Contracts, allows a savings association to enter into employment contracts with its officers and other employees with the specific approval of the board of directors. Savings associations may not enter into contracts that constitute an unsafe or unsound practice. The regulation defines as unsafe or unsound any practice that could lead to a material financial loss or damage. OTS regulation 12 CFR § 563.161 provides that compensation to officers, directors, and employees must be reasonable and commensurate with their duties and responsibilities.

Savings associations may not enter into contracts that constitute an unsafe or unsound practice.

### *Determining Compensation and Directors' Fees*

OTS considers all six CAMELS components rated under the Uniform Financial Institutions Rating System in its review of employment contracts and other compensation arrangements.

OTS generally defers to the savings association's board of directors concerning executive compensation arrangements, provided that the following conditions exist:

- The institution is not in troubled condition.
- The compensation arrangements do not present significant safety or soundness concerns that could lead to material financial loss or damage to the association.
- Members of the board complied with their fiduciary duties in approving the compensation arrangement.

OTS requires the board of directors of each savings association to annually review all employment contracts and compensation arrangements for senior executive officers and directors. The board must also document its justification and approval in board minutes. Directors who have a personal interest in the compensation arrangements should not participate in the deliberations or vote on the arrangements. Renewal or extension of employment contracts requires approval by the board of directors.

In determining the compensation of principal officers, the board of directors should consider at least the following factors:

- The qualifications and experience of the officer.
- The compensation paid to other persons that the association or service corporation employs.
- The compensation paid to persons having similar duties and responsibilities in other insured associations or service corporation affiliates.
- The size of the association or service corporation, and the complexity of its operations.
- The financial condition, especially capital position and income level, of the association or service corporation and the individual's contributions to the association or service corporation.
- Any other amounts the officer receives, either directly or indirectly, for other services performed for the association or service corporation such as fees for serving as appraiser, attorney, escrow agent, insurance agent.
- The value of personnel fringe benefits provided to the employee, and perquisites such as an automobile, club membership, and expense account.

Directors should be keenly aware of their fiduciary responsibilities when they establish fees and benefits for themselves. Each director should keep in mind that a primary responsibility is to establish policies that protect the assets of the association. Thus, in setting its own fees, directors should use factors similar to those used in setting officers' compensation.

The board of directors must also determine and document whether the fees of outside appraisers and attorneys are reasonable and commensurate with the services performed. This is particularly important if the outside appraiser or attorney is an affiliated person. The board should determine whether the fees are comparable to those that other appraisers or attorneys performing similar services charge. The board should also consider the comparative advantages of employing a staff appraiser or attorney to perform appraisal or legal services for the association or service corporation.

### *Unsafe or Unsound Compensation Practices*

OTS generally does not require changes to preexisting contracts in healthy associations. Contract provisions, however, that raise significant safety and soundness concerns will be subject to examination comment or formal enforcement action until the association terminates or modifies the contract. OTS may, on safety and soundness grounds, insist that the board replace unacceptable managers and use its best efforts to renegotiate employment contracts that are excessively burdensome on the association.

OTS reviews compensation provisions in savings associations in troubled condition under the following circumstances:

- During examinations.
- In conjunction with applications that contain compensation arrangements.
- When the association submits employment contracts and compensation payments for review.

You should review, comment, or take other appropriate action to correct unsafe or unsound employment contracts.

OTS considers the guidelines below illustrative examples of unsafe or unsound compensation provisions. Other compensation provisions may also be objectionable depending on individual circumstances. OTS bases these guidelines on safety and soundness concerns that are especially important for savings associations in troubled condition. You must use judgment in the application of the guidelines, taking into account the condition of the association, the reason for the provision, and the materiality of the provision.

The illustrative examples of unsafe or unsound compensation provisions include the following:

- Compensation arrangements that provide incentives contrary to the safe and sound operation of the association. For example, compensation based primarily on short-term operating results may encourage unreasonable risk-taking to achieve short-term profits. The board of directors should closely monitor compensation tied to current operating results.
- Compensation arrangements that significantly exceed compensation paid to persons with similar responsibilities and duties in other insured associations of similar size, in similar locations, and under similar circumstances, including financial health and profitability.
- Contracts that contain automatic renewals or extensions without providing for the board of directors explicit review and approval.
- Contracts that provide for an excessive term. Generally, a term exceeding three years is objectionable.
- Total compensation paid out upon the departure of an employee, regardless of the reason, that exceeds three times the employee's average annual compensation. (The association should not make any payment when termination is for cause.) Total compensation must include payments for the remaining contract term, if applicable, as well as any severance payments. Associations should base average annual compensation on the five most recent taxable years.
- Contracts that do not adequately reflect or define the duties and responsibilities of the employee.
- Compensation programs (including deferred compensation, retirement, and insurance) for independent directors that are not commensurate with their duties, or that jeopardize their

independence. For example, vesting requirements that require an independent director to forfeit previously accrued amounts if they do not serve for a minimum number of years.

- Contracts that the savings association collateralizes or otherwise guarantees, unless one of the following conditions are present:
  - The terms provide that the contract is unenforceable if the association becomes an association in a troubled condition.
  - The regional director approves the contract.

*Note:* Contracts that the holding company guarantees are permissible.

- Contracts that provide for employer reimbursement of costs that employees incurred seeking to enforce employment contract terms in the absence of legal judgment or settlement.
- Change in control provisions that provide for immediate vesting, particularly for savings associations in a troubled condition.
- Contracts that require payment upon the voluntary resignation of the employee.

The foregoing does not apply to employment contracts or other compensation arrangements between a holding company and a holding company executive. OTS does not comment on employment contracts between a holding company and a savings association executive unless such contract or arrangement is likely to adversely affect the financial or managerial condition of the association. If applicable, OTS requires separate employment contracts between a savings association executive and the association, and the savings association executive and the holding company.

Savings associations should include the following golden parachute provision in new and renewed employment contracts. “Any payments made to the employee pursuant to this agreement, or otherwise, are subject to and conditioned upon their compliance with 12 USC § 1828(k) and FDIC regulation 12 CFR Part 359, Golden Parachute and Indemnification Payments.”

## Operating Results

The board of directors is responsible for maintaining an adequate level of capital for the association. See [Examination Handbook Section 120, Capital Adequacy](#). You should be alert to salary increases and dividend payouts in an association experiencing unstable or declining levels of capital or earnings. If an association fails to meet any capital standard, you should question the board of directors and management of the association. They should justify any increases in compensation for principal officers and directors or dividend payouts.

The board of directors is responsible for maintaining an adequate level of capital for the association.



OTS bases its regulatory and supervisory scheme on performance-based standards that tie directly to capital compliance. Well-capitalized, well-managed institutions that do not pose significant supervisory concerns receive significantly less intrusive oversight, including a longer examination cycle.

Presented below are some of the more common restrictions placed on undercapitalized associations or those institutions in troubled condition.

## *Capital Plan*

OTS requires a capital restoration plan when an association falls below its adequately capitalized level. The association must adhere to an OTS approved capital restoration plan and comply with all prompt corrective action restrictions.

## *Capital Distribution Restrictions*

OTS regulation 12 CFR § 563.134, Capital Distributions, establishes limits on capital distributions.

## *Prior Approval of Officers and Directors*

Section 563.560 requires savings associations in troubled condition to provide 30 days prior notice to OTS if the association wishes to add a director or employ a senior executive officer. OTS has the authority to disapprove the addition or employment of the individual within a 30-day period. OTS may extend the 30-day period for an additional period not to exceed 60 days and must notify the individual in writing of the extension.

## *Prior Approval of Employment Contracts*

A savings association in troubled condition must submit all senior executive officer and director employment contracts to the regional director for prior review. The regional director may extend this requirement to other employees of the association as well. Compensation at associations in troubled condition requires regulatory scrutiny on a case-by-case basis. OTS must balance the association's need to lower operating expenses against the need to provide a higher than normal level of compensation to attract and retain qualified management.

## *Golden Parachute Provisions*

FDIC regulation 12 CFR Part 359, Golden Parachute and Indemnification Payments, implements 12 USC § 1821(k). Part 359 prohibits, with certain exceptions, troubled insured institutions from making golden parachute payments.

The FDIC's Part 359 defines a golden parachute payment generally as any payment that meets the following criteria:

- The institution makes the payment to an institution-affiliated party.

- The payment is contingent on this person's resignation.
- The institution makes the payment while it is in troubled condition.

An institution-affiliated party includes any director, officer, employee, or controlling stockholder (other than a depository institution holding company) of, or agent for, an insured depository institution or depository institution holding company. The rule excepts legitimate business expenses such as the following from the golden parachute payment prohibition:

- Qualified retirement plans.
- Nonqualified "bona fide" deferred compensation plans.
- Nondiscriminatory severance pay plans.
- Other types of common benefit plans.
- Certain payments required by state law.
- Death benefits.

The regulation provides for other limited exceptions in cases involving the hiring of a new manager to improve the institution's condition or when the owners sell a troubled institution without FDIC assistance.

### *Regulatory Review of Third-Party Contracts*

A savings association with a composite CAMELS rating of 4 or 5 must first notify and receive Regional Director approval before it enters into third-party contracts for services outside the normal course of business. OTS has particular concerns regarding third-party contracts at troubled associations because they frequently waste scarce resources. The regional director may establish a de minimis threshold amount to apply on a case-by-case basis. The requirement for regional director preapproval does not apply to contracts in the normal course of business, such as annual audits, debt collection, or routine legal services.

Third-party contracts must not contain provisions that are detrimental to the savings association or contrary to public interest. You should scrutinize them closely since the costs may ultimately increase the cost of an association's failure to the

A savings association with a composite CAMELS rating of 4 or 5 must first notify and receive Regional Director approval before it enters into third-party contracts for services outside the normal course of business.

deposit insurance fund. You should use the following guidelines when reviewing such contracts for associations with a composite CAMELS rating of 4 or 5:

- Associations must clearly identify the services the consultant will provide and discuss how they relate to the association's approved business or capital plan.
- The association must provide evidence that fees to be paid and terms of payment are within prevailing market norms and are consistent with the interests of the insurance fund.
- Reimbursable expenses, if provided, should include only necessary costs directly related to the service provided. (OTS does not consider costs such as entertainment and unnecessary travel as reasonable.)
- Each contract must contain a provision stating that the association may cancel for unsatisfactory or nonperformance.
- In most circumstances, associations should enter into only one contract for each service a consultant will perform. OTS generally considers multiple contracts to different providers for the same service to be a dissipation of assets.
- The association must receive written approval from the regional director to enter into a proposed third-party contract.

### Other Requirements

Directors should be ever-mindful of the savings association's obligation to serve the community. Directors represent the association and their behavior can enhance or detract from the association's image and ultimately its fiscal well-being. A director's business and personal affiliations should be compatible with those of the association.

You should be alert to self-serving practices that include:

- Gratuities to directors to obtain their approval of financing arrangements.
- The use of particular services.
- The use of association funds by insiders to obtain loans or transact other business.
- Transactions involving a conflict of interest.

### *Composition of the Board of Directors*

The composition of the board must meet the following requirements of 12 CFR § 563.33:

- A majority of the directors must not be salaried officers or employees of the savings association or any subsidiary or (except in the case of a savings association having 80% or more of any class of voting shares owned by a holding company) any holding company affiliate thereof.

- Not more than two of the directors may be members of the same immediate family.
- Not more than one director may be an attorney with a particular law firm.

Accordingly, boards should be made up of both inside and outside directors, each providing a distinct role:

- *Inside directors* are responsible for approving high-level budgets prepared by upper management, implementing and monitoring business strategy, and core corporate initiatives and projects. Inside directors are either shareholders or high-level management from within the company. Inside directors help provide internal perspectives for other board members.
- *Outside directors* have the same responsibilities as the inside directors in determining strategic direction and corporate policy; however, outside directors are different in that they are not directly part of the management team. The purpose of having outside directors is to provide unbiased and impartial perspectives on issues brought to the board.

### *Conflicts of Interest*

Directors must particularly avoid conflicts of interest of any sort, or even the appearance of a conflict of interest. Also, because a director's personal characteristics may reflect on the association's trustworthiness, a director should be a responsible and trusted member of a community. OTS's regulation on conflicts of interest, 12 CFR § 563.200, prohibits persons who owe a fiduciary duty to a savings association from advancing their own personal or business interests at the expense of the association. This regulation also prohibits persons who owe a fiduciary duty to the savings association from advancing the personal or business interests of others with whom they have a personal or business relationship at the expense of the association.

The following examples are types of transactions that the rule prohibits:

- A person who owes a fiduciary duty to an institution receives money or other benefits (such as a loan, forgiveness of debt, goods or services) from a third party. In return, the third party receives a benefit from the association (such as granting a loan to or buying property from the third party).
- A third party makes payments to a spouse, child, parent, sibling, or business partner of a person identified in the rule. Those payments generally provide a benefit to the person identified in the rule because of the personal or business relationship.
- A person who owes a fiduciary duty to an institution facilitates a transaction between the savings association and companies in which that person owns shares, is on the board of directors, or is an officer, at the expense of the institution.

Generally, OTS will not deem a person to be advancing his, her, or its interests at the expense of the institution if the transaction complies with sections 23A and 23B of the Federal Reserve Act and

Federal Reserve Board Regulation O. In addition, the regulation provides that if persons who owe a fiduciary duty to a savings association have an interest in a matter or transaction before the board they must take the following steps:

- Make full disclosure to the board.
- Refrain from participating in the board's discussion of the matter.
- Recuse themselves from voting on the matter if they are board members.

### TWA's Sister Bank Exemption

One exemption to 23A, the Sister Bank Exemption, exists for transactions between a bank or thrift and another bank or thrift if a company controls 80 percent or more of the voting securities of both banks or thrifts or if one bank controls 80 percent or more of the voting securities of the other. According to the Federal Reserve, such exemptions reflect the fact that, under the cross-guarantee provisions of the Federal Deposit Insurance Act, an insured depository institution is generally liable for any loss incurred by the FDIC in connection with the default of a commonly controlled depository institution. Notwithstanding the cross-guarantee provisions, the board must ensure that all transactions between the thrift and its affiliates are safe and sound, and in the thrift's best interest.

### *Corporate Opportunity*

OTS's corporate opportunity regulation prohibits directors, officers, and persons that have the power to direct the management or policies of a savings association, or otherwise owe a fiduciary duty to an association, from taking advantage of corporate opportunities that belong to the association. OTS follows common law standards governing usurpation of corporate opportunity. The following are examples of issues the board should consider under this standard:

- The institution's financial condition and management resources.
- The level of risk presented by the business.
- Potential profit from the business weighed against any profits that might arise from transfer of the business.

The rule does not apply when an institution receives fair market value consideration for the transfer of a line of business. In addition, the rule does not generally apply if a disinterested and independent majority of the savings association's directorate, after receiving a full and fair presentation of the matter, rejects the opportunity as a matter of sound business judgment. A disinterested director has no interest in the matter or transaction before the board of directors. An independent director must not be a salaried officer or employee of the savings association, any subsidiary or holding company affiliate. In addition, an independent director must not be dominated or controlled by an interested officer or director.

## *Political Contributions and Loans to Political Candidates and Committees*

The board of directors is responsible for authorizing any political activity by a savings association and must ensure that borrowers properly report political loans.

The Federal Election Commission (FEC) administers, interprets, and enforces the Federal Election Campaign Act of 1971 (the Act) as amended (2 USC § 431). The FEC's implementing regulations that govern political contributions and bank and savings association loans are at 11 CFR Part 100.

The Act and the FEC's regulations apply to the political activities of the following entities:

- Federally chartered corporations in connection with any election, whether federal, state, or local.
- Nonfederally chartered corporations in connection with a federal election.

Thus, a state-chartered subsidiary of a federal savings association is usually not subject to the prohibitions governing its federally chartered parent, absent any circumvention of the Act or implementing regulations.

The FEC's rules and regulations prohibit savings associations from making political contributions and paying political expenditures. For federal associations these prohibitions apply to any election, but for state associations the prohibitions apply to federal elections. Directors should consult legal counsel regarding any questionable activities related to political contributions and loans or payment of expenditures to any political candidates or committees.

Besides the Act's requirements and FEC regulations, savings associations may also be subject to state and local political activity laws.

You should report apparent violations and, when appropriate, forward them to your supervisor. OTS may forward the referral to the FEC for enforcement action. You should consider filing a Suspicious Activity Report when a violation is of a serious, knowing, and willful nature.

Associations may direct their requests for FEC advisory opinions to the following address:

Federal Election Commission  
Office of the General Counsel  
999 E Street, N.W.  
Washington, D.C. 20463

## *Foreign Corrupt Practices Act of 1977*

Congress designed the Foreign Corrupt Practices Act (FCPA) (15 USC § 78dd – 1&2) to prevent the use of corporate assets for corrupt purposes. The FCPA makes it a crime for a U.S. company (or individuals acting on behalf of a company) to bribe foreign officials or foreign political candidates or parties to acquire or retain business. There is an exception for generally accepted "grease" payments to

facilitate processing. The FCPA applies to issuers of registered securities and domestic concerns, their officers, directors, agents, and stockholders. Under the FCPA, the company may be criminally liable if it indirectly engages in prohibited acts through any other person or entity, including a foreign subsidiary.

The FCPA also requires the establishment of internal controls to ensure that organizations execute transactions according to management's authorization and properly record the transactions so as not to disguise corrupt payments. Anyone acting on behalf of a savings association, in any transaction with a foreign official, should have benefit of legal counsel to ensure compliance with the far-reaching provisions of the FCPA.

### *Regulation O*

Savings association directors bear a major responsibility in dealing with loans to members of the directorate and other insiders. They must make decisions that preclude the possibility of partiality or favored treatment. Losses that develop from unwarranted loans to an association's insiders or to their related interests weaken the association's general credit standards. See [Examination Handbook Section 380, Transactions with Affiliates and Insiders](#).

### *Reporting of Loans from Correspondent Banks*

Under 12 CFR Part 215 Subpart B requirements, executive officers and principal shareholders and their related interests must submit an annual report to their board of directors regarding their indebtedness to correspondent banks. OTS incorporates this provision in 12 CFR § 563.43.

### *Securities Laws*

Directors of stock associations must take care not to violate federal securities laws in their own securities trading activity. These laws prohibit anyone, insider or not, from purchasing or selling securities with the use of material corporate information that is not available to the general public. Examples of such material inside information include:

- Significant corporate actions.
- Reduced or increased earnings.
- Changes in loan loss reserves.
- Mergers, acquisitions, or proposed tender offers.
- Actual or potential enforcement or supervisory actions.
- A change in supervisory status (such as a prompt corrective action category or a CAMELS rating).

Federal securities laws also prohibit insiders from passing inside information to other persons, even if the insider does not actually trade securities based on such information.

Related to insider trading prohibitions are short swing profit recovery provisions of § 16 of the Securities Exchange Act of 1934 (15 USC § 78c). A “short swing” transaction generally includes purchases and sales, or sales and purchases, of equity securities within a period of six months. Section 16(b) provides that an issuer, or shareholder acting on behalf of an issuer, may recover from an insider any profits realized on certain short swing transactions.

Corporate insiders have a fiduciary responsibility of trust and confidence to refrain from trading based on material nonpublic information concerning their corporation. The misuse of material nonpublic corporate information is a fundamental breach of fiduciary duty and an unsafe and unsound practice.

## Other Areas of Review

### *Management Official Interlocks*

OTS regulations also address management official interlocks and depository interlocks. See OTS regulation 12 CFR Part 563f. A management official of a depository institution or depository holding company may not generally serve as a management official of another depository institution or depository holding company if the two organizations are not affiliated and are very large or located in the same local area.

### *Indemnification Payments*

A federal savings association may indemnify its directors, officers, and employees according to OTS regulation 12 CFR § 545.121. Such indemnification however, is subject to and qualified by 12 USC § 1821(k). This regulation limits the ability of insured institutions to pay the liabilities or legal expenses of a director or employee who is subject to an enforcement proceeding.

Part 359 in the Code of Federal Regulations limits indemnification payments. The rule generally prohibits indemnification payments made to or for an institution-affiliated party in connection with a civil money penalty or judgment resulting from a federal administrative or civil enforcement action instituted by any federal banking agency. The rule also prohibits payment of liability or legal expenses with regard to administrative proceedings or civil actions instituted by any federal banking agency that results in a final order or settlement pursuant to which an institution-affiliated party is:

- Assessed a civil money penalty.
- Removed from office.
- Prohibited from service.
- Subject to various other penalties.



The rule permits institutions to buy commercial insurance to cover expenses other than judgments and penalties. The rule also permits the institution to pay up front for an employee's legal or other professional expenses if the institution's board makes certain findings, and the employee agrees to reimburse the institution if the alleged violation is upheld.

## *Insurance*

### Fidelity Bond Coverage

Savings associations must maintain adequate fidelity bond and directors' and officers' insurance coverage. Directors should periodically review the adequacy of this coverage and carefully review the riders thereto that might impair its utility. The terms of these policies are negotiable. See Section 330, Management Assessment.

Savings associations must maintain adequate fidelity bond and directors' and officers' insurance coverage.

### Life Insurance

It is common practice for savings associations to buy life insurance policies for the benefit of employees. Institutions may also obtain key-person protection for the association. If the beneficiary of the policy is the savings association, refer to [Examination Handbook Section 250, Other Assets/Liabilities](#), for applicable policy and review procedures. If the beneficiary of the policy is the employee, OTS considers the cost of the coverage to be compensation. The board should annually review and approve the policy for reasonableness.

## REFERENCES

### United States Code (2 USC)

The Federal Election Campaign Act of 1971

### United States Code (12 USC)

§ 375b Extensions of Credit to Executive Officers, Directors, and Principal Shareholders of Member Banks (22(h))

§ 1817(a)(3) Reports of Condition

### United States Code (15 USC)

§ 78m Periodical and Other Reports

§ 78dd-1&2 Prohibited Foreign Trade Practices/Foreign Corrupt Practices Act of 1977

§ 1828(k) Authority to Regulate or Prohibit Certain Forms or Benefit to Institution-Affiliate

## Code of Federal Regulations (12 CFR)

### *Chapter II: Federal Reserve Board Rules and Regulations*

Part 215 Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks (Regulation O)

### *Chapter III: Federal Deposit Insurance Corporation Rules and Regulations*

Part 359 Golden Parachute and Indemnification Payments

### *Chapter V: Office of Thrift Supervision Rules and Regulations*

§ 544.5 Federal Mutual Savings Association Bylaws

§ 545.121 Indemnification of Directors, Officers and Employees

§ 552.6-1 Board of Directors

§ 560.130 Prohibition on Loan Procurement Fees

§ 561.18 Director

§ 563.33 Directors, Officers and Employees

§ 563.39 Employment Contracts

§ 563.41 Loans and Other Transactions with Affiliates and Subsidiaries

§ 563.42 Additional Standards Applicable to Transactions with Affiliates and Subsidiaries

§ 563.43 Loans by Savings Associations to their Executive Officers, Directors and Principal Shareholders

§ 563.161 Management and Financial Policies

§ 563.200 Conflicts of Interest

§ 563.201 Corporate Opportunity in Savings Associations

§ 563.555 Notice of Change in Control of Director or Senior Executive Officer

Part 563f Management Official Interlocks

Part 570	Safety and Soundness Guidelines And Compliance Procedures Appendix A, Interagency Guidelines Establishing Standards for Safety and Soundness Appendix B, Interagency Guidelines Establishing Standards for Safeguarding Customer Information
----------	--

## Office of Thrift Supervision Guidance

### *Regulatory and Thrift Bulletins*

RB 3b	Policy Statement on Growth for Savings Associations
TB 13a	Management of Interest Rate Risk, Investment Securities, and Derivatives Activities
TB 23a	Sales of Securities
TB 82a	Third Party Arrangements

### *CEO Memos*

CEO No. 133	Risk Management of Technology Outsourcing
CEO No. 171	OTS' Revised Compliance Self-Assessment Guide (SMAART Compliance Management Strategy)
CEO No. 174	Joint Interagency Statement On Application of Recent Corporate Governance Initiative to Non-Public Banking Organizations
CEO No. 176	Business Continuity Planning Booklet
CEO No. 180	SEC's Final Rule Discussing Reports on Internal Control That May Satisfy Both SEC Requirements and FDIC Part 363 Requirements

### *Other References*

Office of Thrift Supervision, *Directors' Responsibilities Guide* (October 1999)

Office of Thrift Supervision, *Director's Guide to Management Reports* (October 1999)

**This page intentionally left blank**

# Oversight by the Board of Directors Program

---

## EXAMINATION OBJECTIVES

To assess whether the composition of the board of directors provides for sufficient breadth and depth of expertise to ensure adequate oversight of the association's affairs.

To determine whether the board of directors fully understands its duties and responsibilities and is discharging its responsibilities appropriately.

To determine whether the board of directors has adopted adequate policies, procedures, and operating strategies (including internal controls, a compliance management program, and audit and loan review procedures) to conduct the association's operations prudently.

To determine the existence of any conflicts of interest or improprieties involving directors.

To determine the extent of compliance with statutory and regulatory requirements applicable to directors of savings associations.

## EXAMINATION PROCEDURES

### LEVEL I

WKP. REF.

1. Review the association's business plan, budgets, and policy statements. Determine if the board of directors establishes objectives and policies for the association in general and for specific relevant areas of operation. Determine whether objectives and policies are compatible with applicable laws, regulations, the charter or articles of incorporation, bylaws, and conditions for insurance of accounts. Evaluate the adequacy of stated policies in providing direction to management.

---

2. Review board of director's minutes of regular, special, and committee meetings; consider director attendance at the meetings. Determine whether minutes are complete, the extent of significant changes in direction, activities, or policy for the association, and whether specific changes require modification of the scope of the examination. Update the continuing examination file (CEF), if applicable, with new

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Oversight by the Board of Directors Program

---

WKP. REF.

or revised policies (or reference the policies if not retained). You should inform other examiners of noteworthy information found during the review.

---

3. Review reports that management prepares for the board. Determine if the information is adequate, accurate, and sufficient to support the board of director's decision making. (Examiners reviewing related areas can perform this procedure.) Confirm that management's reports adequately address financial and operational risks, including technology risks, and compliance performance. Provide copies of useful board reports and other information to the other examiners.
- 
4. Review and evaluate the composition of the board of directors. Ensure that the association meets the requirements in 12 CFR § 563.33. Obtain answers to the following questions and disseminate information regarding directors' interests to the examination team:
- Is there always a quorum, that is, a majority of the directors that the association's bylaws prescribe, at board meetings?
  - Do the directors, as a group, have sufficient expertise and experience?
  - Are three or more of the association's directors members of the same family? Do related directors tend to control board actions?
  - Do two or more directors also work as attorneys with the same law firm?
  - Could the directors' affiliations have any adverse effects on the association's operations and, if so, would a larger board offset the possible adverse effects?
  - Is there a concentration of board members and, therefore, a concentration of interests in certain businesses (such as real estate or construction)?
- 
5. Determine whether there were any occurrences of self-dealing or conflicts of interest involving the board of directors.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Oversight by the Board of Directors Program

---

WKP. REF.

6. Complete the [General Questionnaire](#), Oversight by the Board of Directors.

---

7. Determine whether the board of directors:

- Delegates sufficient authority to management personnel to promote effective and efficient performance and foster an environment for regulatory compliance, while retaining sufficient control to discharge its responsibilities to stockholders, members, customers, OTS, and other regulatory authorities.
- Is aware of significant regulatory changes enacted during the examination period.
- Actively oversees the association's operations and adequately monitors its performance.
- Provides direction to management as to the development of an optimal risk/return profile.
- Receives a status report on and approves the association's compliance with the Interagency Guidelines Establishing Standards for Safeguarding Customer Information, which implement Section 501(b) of the Gramm-Leach-Bliley Act of 1999.
- Provides sufficient resources for implementing its compliance management program given the association's business strategies, operational complexity, and regulatory obligations.
- Is aware of all the association's funds management procedures, including management's financial modeling processes.
- Provides sound funds management direction to management.
- Reviews and takes appropriate corrective actions to address adverse findings or criticisms disclosed in internal and external audit reports, reports of examinations, and internally generated reports, such as internal asset review reports and compliance self-assessment reports.
- Reviews the level and reasonableness of officers' salaries and confirms that they are commensurate with their experience and duties.

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Oversight by the Board of Directors Program

---

WKP. REF.

- Provides adequate oversight of the personnel department and its policies.
  - Reports annually to the shareholders in the required format, if applicable.
- 

8. Review employment contracts. Be especially alert for contracts with long terms or overly generous provisions. Determine whether the association employs or retains persons closely related to officers and directors. Determine whether such relationships or inappropriate contracts have affected, or could adversely affect, the system of internal control, employee morale, or association performance. Ensure employee contracts meet the requirements of 12 CFR § 563.39.

---

9. Interview the managing officer and other key officers, including the chief financial officer and the chief lending officer. Determine whether they keep directors informed of the association's financial position and the potential effect of current economic conditions on the association. Also determine the extent of the directors participation and involvement in resolving current operating problems and establishing long-range objectives and policies.

---

10. Review Level II procedures and perform those necessary to test, support, and present conclusions derived from performance of Level I procedures.

---

## LEVEL II

1. Obtain answers to the following questions relating to the board of directors:
- Does the board of directors review reports from the executive committee, audit committee, loan committee, other committees of the board, compliance personnel, and outside experts at board meetings?
  - Do directors and committee members have the opportunity to review and modify minutes of their meetings before approval?

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



# Oversight by the Board of Directors Program

---

WKP. REF.

- Are directors aware of significant regulatory changes enacted during the examination period?
- Has the board appointed a compliance officer?
- Has the board adopted and maintained a comprehensive compliance management program predicated on systems, real-time monitoring, periodic self-assessment, organizational accountability, responsiveness to needed improvements, and effective training (OTS' SMAART Compliance Program Components)?
- Did management consider the results of prior years' compliance reviews and examination reports when they designed procedures for the current compliance review
- Did the audit committee or the board review the results of the most recent compliance audit, compliance reviews, and self-assessment reviews?
- Are adequate systems of internal control present to detect noncompliance with regulations?
- Are written responses and plans for corrective action required from management concerning deficiencies noted during the compliance audit, reviews, or self-assessments?

---

2. Did each regular director's meeting during the examination period include a review of financial reports of the association and its affiliates? Also, consider the following:

- Do the minutes reflect directors' questions concerning financial reports along with the appropriate follow-up and resolutions?
- Did the board review recommendations concerning fiscal operations in examination reports and the board of director's letter from independent accountants?
- Did the board approve and prepare written responses to recommendations contained in examination reports and the board of director's letter from the independent accountants?
- Does the board regularly assess or monitor management's compliance with board approved major financial polices?

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Oversight by the Board of Directors Program

---

WKP. REF.

- Do the minutes reflect that the directors thoroughly reviewed and approved the association's budget?
  - Does management include comparisons of budgets with actual results in financial reports reviewed at each board meeting?
- 

3. Did the board establish and do they annually review minimum underwriting standards and guidelines, including a large loan policy? Check the following items:

- Does management establish, and does the board review and approve formal lending limits?
  - In conjunction with the budgeting process and formulation of the business plan, has the board reviewed and approved the types and volume of lending planned by management?
  - Do the association's lending policies require that higher-risk credit extensions and unusual loans (as specifically defined in the policies) be presented to the board for final approval?
  - Do the minutes reflect if the board considered any unusual loans or those exceeding ordinary risk? Do the minutes reflect the board's approval or disapproval?
  - Do the minutes reflect that the board, in reviewing higher-risk loans, explored efforts to minimize risk and limit the amount invested?
  - Has the board implemented an effective internal asset review function?
- 

4. Review the following items:

- Does the board define, in writing, the managing officer's duties and responsibilities?
- Do the directors generally establish and approve compensation levels and pension plans?
- Do directors approve promotions and bonuses and document such approvals in the minutes?

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Oversight by the Board of Directors Program

---

WKP. REF.

- For bonus plans tied to the association's net income, has the board established controls to prevent management from reporting short-term gains at the expense of long-term profitability?
- 
5. Review directors' compensation for reasonableness. Consider peer group information and the time directors devote to the association's affairs.
- 
6. Determine if operating committees are active between board meetings, and if the committees subsequently report their actions to the board for ratification.
- 
7. Review the association's bylaws, charter or articles of incorporation, and conditions for insurance of accounts. (Include copies in the CEF or permanent institution file.) Determine if written policies and procedures specify the duties and responsibilities of management personnel and the board of directors.
- 
8. Review and consider the CAMELS component ratings and the compliance rating in determining your overall conclusions regarding the oversight by the board of directors.
- 
9. Determine if there is a need to review any association transactions for evidence of self-dealing or conflicts of interest.
- 
10. Ensure that your review meets the Examination Objectives of this Handbook Section. State your findings, conclusions, and recommendations for any necessary corrective measures on the appropriate work papers and report pages.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Oversight by the Board of Directors Program

---

WKP. REF.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Oversight by the Board of Directors

### Questionnaire

---

Yes    No

---

#### General Questionnaire

##### ***Board of Directors - General Requirements***

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 1. Does the board implement policies and procedures to ensure an effective system of corporate governance?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the board ensure that executive officers appropriately manage and supervise day-to-day activities?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Is the composition of the board within the guidelines of § 563.33a)?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Have all directors regularly attended directors' meetings during the year?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Does the board of directors regularly review reports from the executive committee, audit committee, loan committee, other committees of the board, compliance personnel, and outside experts at board meetings? | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Has each director had the opportunity to review and modify all minutes of board and committee meetings during the period prior to approval?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Are the minutes complete?   | <input type="checkbox"/> | <input type="checkbox"/> |

##### ***Conflicts of Interest - 12 CFR § 563.200***

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 8. Does the board of directors review each director's business and personal interests to ensure that the director does not advance his interests (or interests of others that the director has a personal or business relationship with) at the expense of the savings association? | <input type="checkbox"/> | <input type="checkbox"/> |
| • Do board members furnish written conflict-of-interest representations annually?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Has any director engaged in any transaction with the association or its affiliates where the director received preferential treatment? (Apply particular emphasis to loan terms and instruments.)   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Has any director engaged in any transaction with the association or its affiliates that give the appearance of a conflict of interest?  | <input type="checkbox"/> | <input type="checkbox"/> |

##### ***Reporting of Loans from Correspondent Banks - 12 CFR Part 215, § 563.43, FIL-82-2000 (FFIEC-004)***

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 9. Does the board of directors review the reports of indebtedness to correspondent banks that executive officers and principal shareholders and their related interests must annually submit to the board? | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

---

**Oversight by the Board of Directors**  
**Questionnaire**

---

Yes    No

---

***Safety and Soundness Standards - 12 CFR Part 570, Appendix A***

10. Does the board of directors and senior managers ensure that the system of internal control operates effectively?  Yes  No
11. Does the association have an internal audit function that is appropriate to its size and the nature, scope, and risk of its activities?  Yes  No

***Standards for Safeguarding Customer Information – 12 CFR Part 570, Appendix B***

12. Did the board of directors approve and oversee the implementation of a written information security program, as required by the Gramm-Leach-Bliley Act (GLBA), Section 501(b)?  Yes  No
- Does the board receive annual reports regarding the status of the information security program, and the institution's compliance with § 501(b) of GLBA?  Yes  No

***Annual Independent Audits and Reporting Requirements - 12 CFR Part 363***

13. This section only applies to associations where total assets at the beginning of the fiscal year are \$500 million or more:
- Has the board of directors established an independent audit committee?  Yes  No
  - Does the committee review with management and the independent public accountant the basis for the reports that 12 CFR Part 363 requires?  Yes  No

***Sarbanes-Oxley Public Reporting Requirements***

**This section only applies to public institutions that are subject to SEC reporting requirements.**

14. Has the institution included in its SEC filing a management report on the company's internal control over financial reporting? *Note: Savings association and savings association holding companies may choose to prepare a single management report that satisfies both the SEC requirement and Part 363 rather than prepare two separate management reports.*  Yes  No
15. Has the institution included an attestation report by the registered public accounting firm regarding management's assessment?  Yes  No

---

**Oversight by the Board of Directors**  
**Questionnaire**

---

Yes    No

***Interest Rate Risk Management Procedures - 12 CFR § 563.176***

16. Does the board of directors (or a designated committee of the board) review the savings association's interest rate risk exposure?  Yes  No
17. Has the board of directors formally adopted a policy for the management of interest rate risk?  Yes  No
18. Does the board of directors periodically receive reports from management regarding implementation of the interest rate risk policy?  Yes  No
19. Does the board of directors review the results of operations at least quarterly and make adjustments as necessary, including adjustments to the authorized acceptable level of interest rate risk?  Yes  No

***Financial Derivatives - 12 CFR § 563.172***

20. Has the board of directors established written policies and procedures governing authorized financial derivatives?  Yes  No

***Supervisory Policy Statement on Investment Securities and End-User Derivatives Activity***

21. Has the board of directors approved major policies for conducting investment activities, including the establishment of risk limits?  Yes  No
22. Does the board of directors review portfolio activity and risk levels, and require management to demonstrate compliance with approved risk limits?  Yes  No

***Interbank Liabilities - 12 CFR § 206.3***

23. Does the board of directors annually review and approve the association's interbank liability policies and procedures?  Yes  No

***Payment Systems Risk - 12 CFR § 210.25***

24. Does the board of directors control the risks of participation in the systems by establishing caps and reviewing policy compliance?  Yes  No

***Real Estate Lending Standards - 12 CFR § 560.101***

25. Does the board of directors, at least annually, review and approve lending policies for extensions of credit secured by real estate?  Yes  No
26. Do the lending policies reflect risk levels that are acceptable to the board and provide clear and measurable underwriting standards?  Yes  No

**Oversight by the Board of Directors**  
**Questionnaire**

- |  | Yes                      | No                       |
|--|--------------------------|--------------------------|
| • Do the institution's lending policies require that higher-risk credit extensions and unusual loans (as specifically defined in the policies) be presented to the board for final approval? | <input type="checkbox"/> | <input type="checkbox"/> |
| • Were unusual loans and those exceeding ordinary risk presented to the board during the period, and did the board record their approval or disapproval in the minutes?                      | <input type="checkbox"/> | <input type="checkbox"/> |
| • In reviewing higher-risk loans, did the board explore efforts to minimize risk and limit the amount invested, and did the directors document their review in the minutes?                  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Does the board review the status of all high-risk loans on a regular basis?  | <input type="checkbox"/> | <input type="checkbox"/> |

***Appraisal Policies and Practices of Savings Associations and Subordinate Organizations - 12 CFR § 564.8, TB 55a***

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 27. Has the board of directors developed, implemented, and maintained appraisal policies to ensure that appraisals reflect professional competence and reliable market value of the collateral? | <input type="checkbox"/> | <input type="checkbox"/> |
| 28. Has the board of directors developed and formally approved written appraisal policies?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 29. Does the board of director's annually review and approve appraisers for compliance with association policies, procedures and reasonableness of estimates?                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 30. Has the board of directors designated one or more persons as the association's environmental risk analyst and assisted in the development of the association's environmental risk policy?   | <input type="checkbox"/> | <input type="checkbox"/> |

***Classification of Assets - 12 CFR § 560.160***

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 31. Does the board of directors ensure that management evaluates and classifies the association's assets on a regular basis in a manner consistent with or reconcilable to OTS's asset classification system? | <input type="checkbox"/> | <input type="checkbox"/> |
|---|--------------------------|--------------------------|

***Written Security Programs - 12 CFR Part 568***

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 32. Has the board of directors developed and implemented written security programs for the association's physical locations? | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

***Report of Condition - 12 USC § 1817(a)(3), TFR Instructions***

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 33. Do two or more members of the board of directors attest to the report? | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|



---

## Oversight by the Board of Directors

### Questionnaire

---

Yes No

#### **Report of Examination - ROE Instructions**

34. Do the directors review the report of examination and sign the Director's signature page for review during the next examination?

#### **Information Technology**

35. Has the board of directors developed, adopted and implemented appropriate policies, practices, procedures, and controls to identify, manage, and mitigate information technology risks within the association's environment?

#### **Business Continuity Planning - CEO Memo No. 176**

36. Has the board of directors developed a comprehensive, institution-wide business continuity plan, appropriate to the size and complexity of the institution that clearly defines how the association can maintain, resume, and recover its operations after disruptions?

- Is the association's business continuity plan tested annually?
- Are the results of the annual testing presented to the board for review and documented in the corporate minutes?

37. Has the board of directors developed and implemented a program to oversee and manage its technology outsourcing relationships?

- Does the vendor management oversight program ensure that contracts with outsourced technology vendors contain language that the service providers implement security programs designed to meet the objective of § 501(b) of GLBA?

#### **Third Party Arrangements – TB 82a**

38. For significant contracts, does the board of directors regularly receive:

- Risk management reports, including contingency plans?
- Performance reports?
- Oversight activity reports?

39. Does the board have a policy that it must approve the third party vendor selection process, and have access to critical information with regard to the third party's activities?

40. Does the board have policies that require management to develop business plans for significant new lines of business or products that identify the planning process, decision making, and due diligence activities in selecting a third party vendor?

41. Does the board adequately document their decisions regarding third party vendors?

**Exam Date:** \_\_\_\_\_

**Prepared By:** \_\_\_\_\_

**Reviewed By:** \_\_\_\_\_

**Docket #:** \_\_\_\_\_

---

**Oversight by the Board of Directors**  
**Questionnaire**

---

Yes    No

---

***Executive Compensation and Employment Contract Oversight - 12 CFR § 563.39***

42. Does the board of directors annually review and approve all employment contracts and compensation arrangements for senior officers and directors?  Yes  No
43. Has the board of directors defined the duties and responsibilities of the institution's managing officer in writing?  Yes  No
44. For those bonus plans tied to the performance of the institution has the board established controls to prevent management from reporting short-term gains at the expense of long-term profitability?  Yes  No
45. If the institution uses employment contracts, do they meet the requirements of § 563.39?  Yes  No

***Bond Coverage for Directors, Officers, Employees, and Agents - 12 CFR § 563.190***

46. Does the board of directors formally approve and annually review and assess the association's standard and supplemental bond coverage?  Yes  No

***Retail Sales of Nondeposit Investment Products - TB 23-2***

47. Only applicable to associations that permit the sale of nondeposit investment products on their premises:
- Does the board of directors ensure that customers receive disclosures about the nature and risk associated with nondeposit investment products?  Yes  No
  - Did the board of directors adopt and does the board of directors periodically update a written statement that addresses the risks associated with the association's sales program?  Yes  No
  - If the association uses a third party that sells or recommends its nondeposit investment products, has the board of directors approved the agreement with the third party?  Yes  No

***Compliance Management Program – SMAART – CEO Memo No. 171***

48. Has the board adopted and maintained a comprehensive compliance management program predicated on systems, real-time monitoring, periodic self-assessment, organizational accountability, responsiveness to needed improvements, and effective training (OTS' SMAART Compliance Program Components)?  Yes  No

---

## Oversight by the Board of Directors

### Questionnaire

---

- |  | Yes                      | No                       |
|--|--------------------------|--------------------------|
| • Does the board approve and note in its minutes the establishment and maintenance of a written compliance program designed to assure and monitor compliance with the <i>Bank Secrecy Act (BSA)</i> (31 CFR Part 103 and 12 CFR 563.177 and 563.180)?.....   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board ensure that the BSA program includes the following at a minimum?.  |                          |                          |
| — a system of internal controls?   | <input type="checkbox"/> | <input type="checkbox"/> |
| — daily coordination and monitoring by a designated individual?  | <input type="checkbox"/> | <input type="checkbox"/> |
| — independent testing of compliance?   | <input type="checkbox"/> | <input type="checkbox"/> |
| — training for appropriate personnel?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>Truth in Lending Act and Regulation Z</i> (12 CFR Part 226)?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy and comprehensive procedures for implementing the <i>Real Estate Settlement Procedures Act and Regulation X</i> , including explanation of the coverage of the regulation, exemptions, disclosure requirements, Section 8 prohibitions and other relevant requirements (24 CFR 3500)? | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy implementing the <i>Home Mortgage Disclosure Act and Regulation C</i> (12 CFR Part 203)?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>National Flood Insurance Act and OTS regulation</i> (12 CFR 572)?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>Equal Credit Opportunity Act and Regulation B</i> (12 CFR 202)?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>Fair Housing Act</i> (42 USC 3601 et seq.) and implementing HUD regulations (24 CFR 100 et. seq.) and OTS's non-discrimination regulations at 12 CFR 528.9?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>Electronic Fund Transfer Act and Regulation E</i> (12 CFR Part 205)?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>Expedited Funds Availability Act (Regulation CC at 12 CFR Part 229)</i> ?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>Truth and Savings Act and Regulation DD</i> and establish procedures addressing relevant activities (12 CFR Part 230)?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Did the board adopt a policy for implementing the <i>CRA Sunshine</i> regulations (12 CFR Part 533)?   | <input type="checkbox"/> | <input type="checkbox"/> |

**Exam Date:** \_\_\_\_\_

**Prepared By:** \_\_\_\_\_

**Reviewed By:** \_\_\_\_\_

**Docket #:** \_\_\_\_\_



## APPLICABILITY OF SELECTED SARBANES-OXLEY ACT REQUIREMENTS TO FINANCIAL INSTITUTIONS

*Note: Institutions that meet more than one audit category should default to the first listed category (highest category in the hierarchy established in this chart.) For example, a public company that is also subject to FDICIA would be required to comply with all titles in Sarbanes-Oxley and default to the public company category.*

Institution's Audit Category	Title II – Auditor Independence <sup>1</sup>	Title III – Corporate Responsibility <sup>1</sup>	Title IV – Enhanced Financial Disclosure <sup>1</sup>
<b>Public companies</b> <sup>2</sup>	<u>Required</u> <sup>1</sup>	<u>Required</u> <sup>1</sup>	<u>Required</u> <sup>1</sup>
<b>FDICIA required audits</b> <sup>3</sup>	Institutions are <u>required</u> to comply with Sections 201, 202, 203, and 206. Section 204 does not apply under the existing audit standards, but the FDIC may amend Part 363 to encompass standards that mirror Section 204. <sup>6,7</sup>	Institutions are <u>not required</u> to comply with Section 301; however, they must have an audit committee that is independent of management. Institutions are <u>not required</u> to comply with Section 302. Institutions are <u>not required</u> to comply with Section 303 but it is an unsafe and unsound practice to exercise improper influence on the conduct of an audit. <sup>7</sup>	Institutions are <u>not required</u> to comply with Sections 401, 402, 404, and 406. However, the FDIC may amend Part 363 to require compliance with those sections.  Institutions are <u>not required</u> to comply with 407; however, institutions with more than \$3 billion in assets <u>are required</u> to have at least two members of the audit committee with banking or related financial management expertise. The audit committee must have access to its own outside counsel. <sup>7</sup>  When subject to both Section 404 and FDICIA requirements, institutions may chose to prepare one report to meet both requirements or separate reports for the FDIC and SEC. <sup>8</sup>
<b>OTS required audits</b> <sup>4</sup>	Independent public accountants are <u>required</u> to meet the independence requirements and interpretations of the SEC and its staff. <sup>9</sup>	Institutions are <u>encouraged</u> to periodically review their policies and procedures relating to corporate governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. <sup>10</sup>	Institutions are <u>encouraged</u> to periodically review their policies and procedures relating to corporate governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. <sup>10</sup>

**Footnotes are on page 6.**

***Highlights of Selected Sarbanes-Oxley Act Requirements are on pages 3-5.***

Institution's Audit Category	Title II – Auditor Independence <sup>1</sup>	Title III – Corporate Responsibility <sup>1</sup>	Title IV – Enhanced Financial Disclosure <sup>1</sup>
<p><b>All other audits <sup>5</sup> - supervised by OTS, FRB, or OCC.</b></p>	<p>An institution <u>may be required</u> by another law or regulation, an order, or another supervisory action to have its financial statements audited by an independent public accountant. If warranted for safety and soundness reasons, the institution's primary federal regulator <u>may require</u> that the institution and its independent public accountant comply with the auditor independence requirements of Section 201. <sup>6,9</sup></p>	<p>Compliance <u>may be required</u>. If not so required, institutions are <u>encouraged</u> to periodically review their policies and procedures relating to corporate governance and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. <sup>10</sup></p>	<p>Institutions are <u>encouraged</u> to periodically review their policies and procedures relating to corporate governance, internal controls, and auditing matters. This review should ensure that such policies and procedures are consistent with applicable law, regulations, and supervisory guidance and remain appropriate in light of the institution's size, operations, and resources. <sup>10</sup></p>
<p><b>All other audits <sup>5</sup> - supervised by FDIC.</b></p>	<p>Compliance <u>not required</u>. However, institutions are <u>encouraged</u> to follow the internal audit outsourcing prohibition in Section 201, audit partner rotation and "time out" periods similar to Section 203, institute auditor reporting practices similar to Section 204, and to comply with the conflicts of interest requirements in Section 206 given the institution's size, complexity, and risk profile. <sup>7</sup></p>	<p>Compliance <u>not required</u>. However, institutions are <u>encouraged</u> to establish an audit committee consisting entirely of outside directors, similar to Section 301, <u>asked to consider</u> implementing Section 302, and <u>strongly encouraged</u> to comply with Section 303 (improper influence over external auditing work). <sup>7</sup></p>	<p>Institutions are <u>encouraged</u> to implement to the extent feasible given the institution's size, complexity, and risk profile. Institutions are <u>encouraged</u> to implement Sections 401, 404, and 406, and <u>continue to comply</u> with Section 402 (Regulation O). <sup>7</sup></p>

Footnotes are on page 6.

*Highlights of Selected Sarbanes-Oxley Act Requirements are on pages 3-5.*

---

## HIGHLIGHTS OF SELECTED SARBANES-OXLEY ACT REQUIREMENTS

### Title II – Auditor Independence

#### Section 201: Services outside the scope of practice of auditors

- Prohibits the external auditor from providing specified nonaudit services (impermissible nonaudit services) contemporaneously with the external audit. Impermissible nonaudit services include:
  1. Bookkeeping or other services.
  2. Systems design and implementation.
  3. Appraisal or valuation services.
  4. Actuarial services.
  5. Internal audit outsourcing services.
  6. Management functions or human resources.
  7. Broker/dealer, investment advisor or investment banking services.
  8. Legal services.
  9. Expert services unrelated to the audit.
  10. Other services, as the Board deems impermissible.

#### Section 202: Pre-approval requirements

- Audit committee must preapprove all services that are not prohibited that the external auditor provides, including audit, tax services, and other permissible nonaudit services. Some institutions may not have an audit committee, but would instead use the board of directors.

#### Section 203: Audit partner rotation

- The lead or coordinating audit partner and the reviewing partner rotate off the audit every five years with a five-year “time out.” Other significant partners subject to seven-year rotations with two-year “time outs.”

#### Section 204: Auditor reports to the audit committee

- The external auditor must report the following to the company’s audit committee:
  - Critical accounting policies and practices;
  - Alternative accounting treatments under GAAP for material items, including:
    - ♦ The ramifications of the use of alternative treatments, and
    - ♦ The treatment preferred by the auditors; and
  - Other material communications between the auditor and management.

#### Section 206: Conflicts of interest

- A registered public accounting firm may not perform an audit for an institution if a person in a financial oversight role of the issuer (e.g., CEO, controller, CFO, or chief accounting officer, etc.) was a member of the audit engagement team (> 10 hours) of the issuer during a one-year “cooling off” period prior to initiation of the new audit.

---

**Section 208 Audit Disclosures**

- Fee disclosures grouped into the following four categories:
  - Audit fees.
  - Audit-related fees (e.g. employee benefit plan audits, merger and acquisition due diligence, etc.).
  - Tax fees.
  - All other fees.
- Qualitative disclosure of services provided.

**Title III - Corporate responsibility**

**Section 301: Public company audit committees**

- Audit Committee vested with responsibility for the appointment, compensation, and oversight of the external audit firm.
- All members of the audit committee must be a member of the board of directors and be independent. The institution must fund the committee adequately and the committee must be able to hire independent counsel and other advisors.

**Section 302: Certifications**

- Each annual report and quarterly report must include various certifications by the CEO and CFO:
  - That the financial statements and information “fairly present in all material respects the financial condition and results of operations...”
  - That they are responsible for establishing and maintaining internal controls.

**Section 303: Improper Influence on Conduct of Audits**

- Prohibits any officer or director (or anyone under their direction) from taking any action to fraudulently mislead an auditor for the purpose of rendering a financial statement that is materially misleading.

**Title IV - Enhanced financial disclosure**

**Section 401: Disclosures in periodic reports**

- Financial reports must reflect all material correcting adjustments.
- Annual and quarterly reports must disclose material off-balance-sheet transactions and other relationships with unconsolidated entities.

**Section 402: Enhanced Conflict of Interest Provisions**

- Limits personal loans to directors and executive officers.

**Section 404: Management assessment of internal controls**

- Annual reports must contain an internal control report.
  - Must disclose material weakness(es)
  - Management **cannot** conclude internal controls are effective if material weakness(es) exist.
- Can issue one combined report or separate FDICIA and SOX §404 reports.
- Internal control report that meets Part 363 may in some instances be filed with the SEC. Part 363 (FDICIA) requires:
  - A statement of management’s responsibility for preparing the institution’s annual financial



statements, for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and for complying with designated laws and regulations relating to safety and soundness.

— Management’s assessments of:

- ♦ The effectiveness of the institution’s internal control structure and procedures for financial reporting as of the end of the fiscal year, and
- ♦ The institution’s compliance with the designated safety and soundness laws and regulations during the fiscal year.

**Section 406: Code of ethics for senior financial officers**

- Requires that period reports disclose whether the issuer has adopted a code of ethics for senior officers, and if not, why not.
- Requires disclosure of any changes or waivers of the code of ethics.

**Section 407: Disclosure of audit committee financial expert**

- Periodic reports must disclose whether the audit committee has at least one member who is a “financial expert” (and identify).

**Section 906: Certifications**

- Each annual report and quarterly report must include a certification by senior corporate officers:
  - That the financial statements and information “fairly present in all material respects the financial condition and results of operations...”
- Note that this certification is in addition to the one required in Section 302. Section 906 is an amendment to the federal criminal law.

### Footnotes

- <sup>1</sup> Highlights of Selected Sarbanes-Oxley Act Requirements (Pages 3-5 of this document).
- <sup>2</sup> Public companies: Banks, savings associations, and holding companies that have a class of securities registered with either the SEC or the federal banking agencies (including OTS) under Section 12 of the Securities Exchange Act of 1934 or are required to file reports with the SEC under Section 15(d) of that Act (commonly referred to as “public companies”); or, file with OTS pursuant to a reporting obligation under Section 563g.18, and, are required to have an external audit.
- <sup>3</sup> FDICIA required audits: Banks and savings associations with assets of \$500 million or more that are subject to the FDIC’s external audit and reporting requirements under 12 CFR Part 363.
- <sup>4</sup> OTS required audits: Savings associations and savings association holding companies required by OTS to have an audit pursuant to 12 CFR 562. Includes audits of:
- Savings associations with composite CAMELS rating of 3, 4, or 5;
  - Savings association holding companies that control savings association subsidiary(ies) with aggregate consolidated assets of \$500 million or more;
  - *De novo* savings associations; and
  - Other audits deemed necessary for safety and soundness reasons.
- <sup>5</sup> All other audits include: Banks, savings associations, and holding companies that are (1) required to have an audit by another law or regulation, an order, or another supervisory action, warranted for safety and soundness reasons; and (2) not required to have an external audit, but do so.
- <sup>6</sup> Interagency Policy Statement on the Internal Audit Function and Its Outsourcing (March 17, 2003).
- <sup>7</sup> FDIC Financial Institution Letter (FIL) – 17 – 2003, Corporate Governance, Audits and Reporting Requirements (March 5, 2003).
- <sup>8</sup> SEC’s Final Rule Discussing Reports on Internal Control That May Satisfy Both SEC Requirements and FDIC Part 363 Requirements, OTS CEO Letter No. 180 (August 21, 2003).
- <sup>9</sup> Section 102 of the Sarbanes-Oxley Act requires audits of public companies to be performed by PCAOB “registered” accountants. This requirement does not apply to nonpublic companies. Auditors of nonpublic institutions must follow the independence standards identified in the AICPA Code of Professional Conduct.
- <sup>10</sup> Joint Interagency (OTS, FRB, OCC) Statement on Application of Recent Corporate Governance Initiatives to Nonpublic Banking Organizations, OTS CEO Letter No. 174 (May 5, 2003).

## Management Assessment



One of the most important examination objectives is to evaluate the quality and effectiveness of management. The success or failure of almost every facet of operations relates directly to management. Assessments of the various areas under review during an examination all reflect ultimately on the effectiveness of management. Among other things, management is responsible for:

- Implementing board established policies and strategic goals.
- Identifying and managing risk through an effective risk management function.
- Ensuring an effective system of internal controls and management reporting.
- Ensuring the adequacy and depth of resources.
- Ensuring compliance with laws and regulations.
- Ensuring the overall safe and sound operation of the institution.

In this Section, management refers to executive officers, such as chief executive officer, president, vice presidents, chief financial officer, treasurer, controller, secretary or any other person, including division managers, who have the ability, with or without explicit authority, to implement and interpret the association's strategic goals and policies.

---

**L I N K S**

-  [Program](#)
-  [Questionnaire](#)

In evaluating management, you should consider the knowledge, skills, and abilities of the executive officers, their track record, regulatory compliance, and financial performance of the institution. Sound compliance management is a major consideration when evaluating the quality and effectiveness of the board and management. An effective compliance management function should include a process for assessing and monitoring compliance performance, training, and for implementing corrective action based on identified deficiencies. You should consider determinations made in each of the core examination areas (Capital, Asset Quality, Earnings, Liquidity, Sensitivity, Compliance) in your overall assessment of management.

The management rating for a given examination clearly reflects all of the examination findings in a comprehensive examination as well as:

- A demonstrated willingness and ability to serve the banking needs of the community
- Avoidance of conflicts of interest and usurpation of corporate opportunity
- Good corporate governance
- Responsiveness to recommendations for corrective action
- Risk management and financial performance
- Compliance management.

## EFFECTIVENESS OF MANAGEMENT

Assessing management performance involves more than noting whether an association is profitable. Effective management requires the cooperation and active involvement of both management and the board of directors. The board should provide the guidelines, and management should make operating decisions consistent with the guidelines. You must judge management performance on the basis of how well management uses available resources to accomplish the association's objectives.

Effective management requires the cooperation and active involvement of both management and the board of directors.

Evaluations of management provide indicators of future operations; in some instances they may reveal a need for preventive supervision. For associations experiencing problems, evaluations are necessary to determine the capabilities of management so that you may initiate appropriate supervisory action.

OTS has determined that inefficient, incompetent, or dishonest management are the principal causes for the problems of most troubled associations. Although there are many other reasons (high expenses, poor lending practices, high delinquencies, and so on), most of the causes ultimately relate to management deficiencies.

In reviewing executive officers' performance, you need to determine that the following conditions exist:

- Sound corporate governance policies including conflict of interest and corporate opportunity policies.
- Sound and consistent objectives, policies, and procedures in the asset, liability, and operational areas, including information technology and customer information security.
- The timely identification, assessment, and mitigation of risk.
- The ability, knowledge, and attitude to manage compliance responsibilities.
- Personnel throughout the association adhere to policies and receive training ensuring clear communication of relevant legal and regulatory requirements, and procedural guidelines.
- A strong system of internal controls, including technology risk controls.

- Management information systems facilitate efficient operation and ensure effective communications and monitoring of activities.
- The association's planning processes facilitate achievement of goals and objectives. The planning process includes business continuity and disaster recovery.
- Senior management delegates appropriate authorities to middle management and staff personnel.
- Management's experience and depth ensures sound decisions and assures continuity of operations.
- Management is capable of handling situations the association may reasonably encounter in the future.
- Track record, including track record in remedying previously identified problems.

## Risk Management

Risk management—that is the timely identification, assessment, and mitigation of risk—is an integral part of management's responsibilities. An effective risk-management framework identifies potential events that may affect the institution and establishes how an institution will manage its risk given its risk appetite and strategic direction. A risk management program should be consistent with the size, complexity, and risk profile of an association.

In evaluating risks, managers need to consider both current and planned or anticipated operational and market changes and identify the risks arising from those changes. Once risks have been identified, assessed and evaluated as to their potential impact on the organization, management must determine the effectiveness of controls and develop and implement additional appropriate mitigating controls where needed. The effectiveness of those controls should be evaluated independently of the group that develops the controls.

Traditional risk management has focused on quantifiable risks, such as credit and market risks. Recent events have demonstrated the need for greater focus on the risks that are harder to quantify—that is, operational, legal, and reputation risks. A strong regulatory compliance program is an integral part of the risk-management function. The compliance area is critical to identifying, evaluating, and addressing legal and reputation risks, particularly in complex financial firms.

## Safety and Soundness and Compensation Standards

Appendix A of 12 CFR Part 570, entitled Interagency Guidelines Establishing Standards for Safety and Soundness, sets forth operational and managerial standards for insured associations to follow with respect to the following activities and practices:

- Internal controls and information systems (includes controls and systems for compliance)
- Internal audit systems
- Loan documentation
- Credit underwriting
- Interest rate exposure
- Asset growth
- Asset quality
- Earnings
- Compensation, fees, and benefits.

The compensation guidelines require associations to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the association.

Appendix B of 12 CFR Part 570, entitled Interagency Guidelines Establishing Standards for Customer Information, sets forth administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. An association must:

- Implement a board-approved, written information security program.
- Conduct and document a risk assessment of customer information security.
- Require in contracts that service providers implement security programs designed to meet the objectives of this section.
- Monitor, evaluate, and adjust for changes within the association.
- Report to the board annually on the association's compliance and status of the program.

The compensation guidelines require associations to maintain safeguards to prevent the payment of compensation, fees, and benefits that are excessive or that could lead to material financial loss to the association. The guidelines define compensation to be excessive when it is unreasonable or disproportionate to the services that an executive officer, employee, director or principal shareholder performs, in consideration of the following factors:

- The combined value of all cash and non-cash benefits provided to the individual.
- The compensation history of the individual and other individuals with comparable expertise at the association.

- The financial condition of the association.
- Comparable compensation practices at comparable associations.
- For post-employment benefits, the projected total cost and benefit to the association.
- Any connection between the individual and any fraudulent act or omission, breach of trust or fiduciary duty, or insider abuse with regard to the association.
- Any other factors the federal banking agencies determine to be relevant.

Section 570.2(b) provides that if OTS determines that an association fails to meet a safety and soundness standard, OTS may request the submission of a safety and soundness compliance plan.

Regulatory Bulletin 27b provides compensation provision guidance and clarifies OTS policy about unsafe and unsound practices relating to executive compensation and employment contracts.

### Compliance Management Program

Sound compliance management, like other areas of operations management is predicated on establishing a comprehensive program of risk controls, periodic reviews, and self-assessments. Actively managing compliance risk starts at the board of directors' level through senior and middle management down to staff personnel.

Your assessment of management's performance in compliance management should focus on their compliance management program and how well it addresses components the agency expects in a comprehensive program: systems, monitoring, assessment, accountability, response, and training (SMAART components).

In assessing the board and management performance in compliance management, consider the following factors:

- Management allocates sufficient resources for the implementation of a formal written compliance program tailored to its size, organizational structure, business strategy, complexity of operations, market products offered, and staff expertise. The program should:
  - Emphasize the importance of regulatory compliance as an inherent part of business operations.
  - Establish standards of accountability for all personnel charged with compliance-related responsibilities.
  - Include the means for the board and management to actively assess compliance performance.

- The compliance management program provides for and results in:
  - Comprehensive policies and procedures, and the systems to implement them.
  - Internal controls that afford ongoing monitoring to ensure transactions are executed in accordance with program standards.
  - Periodic reviews of systems records and operations to identify transactional violations and program deficiencies.
  - Prompt correction of compliance violations or deficiencies identified during ongoing monitoring, the internal review process or in response to consumer complaints.
  - An ongoing comprehensive training program that ensures the clear communication of relevant legal and regulatory requirements, and the association's procedural guidelines to all affected officers and staff personnel.

### Internal Controls

Both the directors and senior management have important roles in an association's programs of internal control, loan review, internal audit, and compliance management. Although directors have overall audit responsibility and should require that the auditor report directly to them, directors normally charge senior management with the duty of developing and maintaining a strong system of internal controls, including technology risk controls, and a formal compliance management program. Relying on the independent auditors to establish the association's internal controls is inappropriate. Senior management is responsible for the design and implementation of effective controls to prevent errors, conflict of interest situations, and fraud. Refer to Sections [340](#), [341](#), [355](#), and [360](#) of the Examination Handbook.

### Management Information Systems

An effective management information system (MIS) contains information from a number of sources. Such information must serve a number of users, each having varying needs. The MIS must selectively update information from all available sources and coordinate it into meaningful and clear formats. You can determine the effectiveness of MIS on the basis of the following measurements:

- **Quality.** This relates to the relevance and accuracy of the information. Poor quality information usually stems from inadequate controls, analysis, and evaluations of information needs, or from ineffective design of reports.
- **Quantity.** Too many reports or too much information on a single report may hamper or discourage their use completely. Too little information may reflect insufficient analysis of information needs.



- **Timeliness.** The improper design of information processes and the failure to identify the frequency of need for information usually causes untimely processing and distribution of information.

### Prompt Corrective Action

Undercapitalized and significantly under-capitalized associations that fail to submit and implement an acceptable capital restoration plan are subject to the prompt corrective action provisions of § 38(f)(2)(F) of the FDIA. That section permits OTS to dismiss any director or senior executive officer that held office for more than 180 days immediately before under-capitalization. The section also requires the association to employ qualified senior executive officers. Section 38(i)(2)(f) of the statute requires OTS to take action to prohibit critically undercapitalized associations from paying excessive compensation or bonuses.

Also, the prompt corrective action provisions of OTS regulation 12 CFR §565.6(a) impose restrictions on management fees and senior executive officer compensation. Undercapitalized, significantly undercapitalized, and critically undercapitalized savings associations are subject to the management fee provisions of § 38(d) of the FDIA. Significantly undercapitalized and critically undercapitalized associations are subject to the senior executive officer compensation provisions of § 38(f)(4).

Section 38(d)(2) of the FDIA prohibits associations from paying a management fee to any person having control of the association if after the payment the association would be undercapitalized. Section 38(f)(4) provides that undercapitalized or significantly undercapitalized associations that fail to submit and implement an acceptable capital restoration plan shall not do either of the following without prior OTS approval:

- Pay a bonus to a senior executive officer.
- Compensate a senior executive officer at a rate exceeding the officer's average rate of compensation for the year prior to the month when the association became undercapitalized.

### Notice of Change of Senior Executive Officers

OTS regulations 12 CFR § 563.550 through § 563.590 require capital deficient or troubled savings associations to notify OTS 30 days before taking either of the following actions:

- Employing a senior executive officer.
- Changing the responsibilities of any senior executive officer so that the person would assume a different senior executive position.

The same regulatory notice requirement also applies to savings and loan holding companies in a troubled condition.

Capital deficient associations meet one of the following conditions:

- Do not comply with all minimum capital requirements.
- OTS notifies the association, in connection with their capital restoration plan, that it must file a notice.

OTS will disapprove a notice if, based on the competence, experience, character, or integrity of the proposed senior executive officer, that it would not be in the best interests of the depositors or the public to permit the association to employ the individual.

## PLANNING

Sound planning is fundamental to effective management and is a key to anticipating and dealing with rapid change, and managing risk. Senior management and the board of directors should inventory the association's resources, examine changes in its operations, monitor changes in external factors, including legislative, regulatory, industry and, market conditions on its compliance program, and determine its responses to those changes. To be effective, planning should be dynamic in nature. The savings association should carefully monitor and support the planning function. Management must revise projections periodically as circumstances change and the board formulates new strategies to meet stated objectives.

Sound planning is fundamental to effective management and is a key to anticipating and dealing with rapid change.

Planning requires the collection and coordination of large amounts of information and the thoughtful efforts of all members of the management team. Written plans help ensure that the board of directors, executive officers, and all division managers within the association share the same goals, objectives, and strategies. A common and shared perception of future actions is critical to the execution of a successful plan.

Any of the following management failures warrants the attention of the association's directors. You should accordingly note such failures in the report of examination:

- Lack of a satisfactory strategic and operational planning process.
- Failure to develop a comprehensive, association-wide business continuity plan.
- Lack of adherence to plans.
- Ineffective monitoring and control of plans.
- Failure to adjust existing plans to recognize and conform to changing economic and market conditions, legislative and regulatory requirements.

You should also be alert, particularly with respect to new associations, for any deviations to strategic or operational plans that may be potentially detrimental to the association. Such deviations, which you

should also note in the report of examination when assessing management performance, include the following examples:

- The excessive use of or reliance on brokered deposits.
- The initiating of new, novel, or higher risk lending, investment programs, or new technology without appropriate planning, expertise, or controls.
- The failure to independently and adequately investigate and document extensions of credit, particularly those made outside an association's normal lending territory.
- The willingness to forgo long-term stability in favor of short-term profits.
- Many newly chartered savings associations are subject to approval conditions, usually contained in the director's order. You should carefully review the association's adherence to these conditions.

### The Planning Process

To be effective, planning requires a structure and a process. Planning can be segmented into two categories: **strategic** and **operational**. Strategic planning focuses on the long-term, extensive allocation of resources to achieve corporate goals and objectives. Operational planning, such as a business plan, concentrates on shorter-term actions designed to implement those strategies outlined in the strategic planning process. For an effective planning process, the operational plans must flow logically from the strategic plan.

### Management Succession

You should evaluate the association's quality of plans for maintaining its present condition and for improving its future condition. This should include an evaluation of the board and management's efforts to provide for succession of senior officers.

The projection of future management needs involves an appraisal of the quality and quantity of senior and middle management. This assessment must be relative to the size, complexity, and market circumstances of the association. Determination of what management will do with the association in the future is most important. The supervisory goal is to prevent problems from developing rather than wait for future examinations or monitoring to identify deteriorating conditions.

### Regulatory Concerns

You should not evaluate association planning with the preconception that every association should have a model planning process. You should evaluate the planning process and the plan itself. If a well-designed planning process exists, the plan will generally be thoughtful and realistic. Management's

failure to have a satisfactory planning process warrants the attention of the association's directors and you should accordingly report the failure in the report of examination.

You must treat an association's strategic, operational, and business plans with maximum confidentiality. They contain sensitive information that directly affects the association's market position and financial condition.

## MANAGEMENT OF HUMAN RESOURCES

People are the link between an association's organizational structure and the attainment of its organizational goals. The board of directors is responsible for employing a competent chief executive officer. Thereafter, senior management is responsible for recruiting and making certain that there are competent employees available to staff all positions. Personnel management includes establishing procedures for promoting and replacing employees, reviewing their performance, devising a system of compensation, and selecting and training future managers.

The following areas warrant your particular attention in evaluating personnel management, as they are important indicators of an association's viability:

- Detailed position descriptions and standards.
- Carefully planned recruiting and proper screening of new employees.
- Appropriate security training for protecting the association's customer information.
- Performance review and comparison to standards.
- Salary administration.
- Provision for communication.

You should determine the appropriateness of an association's employment contracts, bonus and incentive plans, salary levels, and employee benefits program. You should compare compensation paid and benefits provided with those that an appropriate peer group offers, and should determine reasons for any substantial differences.

## Use of Consultants and Outsourcing

It is fairly common for savings associations to outsource certain functions of the association. Outsourcing functions can reduce operating expenses; however, associations should be careful not to rely on vendors or consultants to perform critical functions without adequate controls. These controls should include monitoring performance as it relates to products and services delivered by or performed on behalf of the association. Monitoring controls are management's first line of defense against operational risk and compliance risk. Use of a vendor or consultant does not lessen the burden on

management to supervise and control the association's systems, policies, and procedures. Management must obtain complete information for vendors and consultants. This should include performing regular due diligence when retaining the services of any third-party provider, vendor or consultant. The savings association must have a written agreement with the vendor or consultant that outlines the conditions, rights, and responsibilities of each party. See Thrift Bulletin (TB) 82a, Third-Party Arrangements.

## AVOIDANCE OF CONFLICTS OF INTEREST

The phrase conflict of interest refers to any situation where the safety and soundness or opportunity of an association is in conflict with the personal interests of any of the following persons:

- A director.
- An officer.
- Any other employee or person who has influence over an association's policies, procedures, or actions.

Conflicts of interest (or even the appearance of such) can compromise safe and sound operations and reputation for integrity. Conflicts can undermine public confidence in the thrift industry.

Sometimes those who owe a fiduciary duty to an association subtly disguise a conflict, making it difficult to detect. In other instances, they may openly acknowledge a conflict. Some conflicts may be detrimental while others may appear to be beneficial to the association. Where a conflict exists, however, its very appearance alone could damage an association's image. A conflict could cause a financial loss to an association if the individual involved considers self-interest and personal gain more important than an association's interests.

Management has a fiduciary responsibility to avoid any conflicts of interest or appearance of conflict of interest. Personal affiliations should not be incompatible with those of the association. Furthermore, when both of the following circumstances exist, no officer should take advantage of a business opportunity for his or her own or another person's personal benefit:

- The opportunity is within the corporate powers of an association or its service corporation(s).
- The opportunity is of present or potential advantage to the association.

Management has a fiduciary responsibility to avoid any conflicts of interest or appearance of conflict of interest.

You should review the association's formal policy for avoidance of conflict of interest situations. The policy at a minimum should address the following concerns:

- Areas where conflicts of interest and usurpations of corporate opportunity could arise. This includes transactions involving the association and persons related to directors or officers, or transactions for their benefit.
- Controls that the association maintains to avoid abuses and the procedures in place for dealing with policy violations.
- Business activities in which the association's directors and senior management are active.
- Business activities that the law permits the association to conduct.
- A specific plan for dealing with conflicts of interest and corporate opportunity problems in these areas.

You should determine if directors and officers are complying with the policy. Accordingly, you should comment on and take appropriate action on any actual or apparent conflict of interest transactions that adversely affect the association, even though an OTS regulation may not specifically address the conflict. Also, you should include comment, and supervisory objection taken, whenever any person involved in the conflict participates in the approval of the subject transaction.

### Loans to Executive Officers

You should have knowledge of Federal Reserve Board Regulation O, 12 CFR Part 215, and OTS regulation 12 CFR § 563.43. Regulation O governs member bank extensions of credit to executive officers, directors, and principal shareholders. Section 563.43 applies the Regulation O restrictions to savings associations. See [Examination Handbook Section 380, Transactions with Affiliates and Insiders](#).

### *Management Questionnaire*

The Preliminary Examination Response Kit (PERK) Management Questionnaire is an important and useful tool in determining objectives and strategies for conducting an examination. In this regard, much of the information that the questionnaire asks for may provide leads in determining the existence of possible conflict of interest situations or transactions. The Management Questionnaire deals with transactions or arrangements with affiliates or affiliates persons, tie-in arrangements, and ownership and control concerns.

You must satisfy yourself as to the completeness and accuracy of responses to the Management Questionnaire, and must follow up on and report any inconsistencies between the responses and your examination findings.

### RESPONSE TO SUPERVISION

You must determine the association's compliance with conditions of approval, orders, supervisory agreements, and directives. Supervisory authorities look to management to implement corrective action

in response to directors' requests and regulatory supervision requirements. Management should establish procedures to ensure continuing compliance. Corrective action must be responsive to the cited criticism and implementation of appropriate action must be timely. Management must explain any noncompliance with supervisory requirements, including plans for corrective action.

If management or the board of directors continues to operate in an unsafe and unsound manner, supervision may have to initiate formal enforcement action. See [Examination Handbook Section 370, Enforcement Actions](#). Your regional Confidential Individual Information System (CIIS) administrator should record the inclusion of any formal enforcement action against an individual in CIIS. The following are some other types of management or director's actions that your CIIS administrator should record in CIIS:

- Criminal referrals.
- Referrals to a professional group for disciplinary purposes.
- Significant business transactions between an association and an individual that raises supervisory concern.

You should contact your regional CIIS administrator for guidance as to whether a particular event warrants an individual's inclusion in CIIS.

## FIDELITY BONDS AND DIRECTORS' AND OFFICERS' LIABILITY INSURANCE

### Fidelity Bonds

Fidelity bond coverage insures against losses attributable to dishonest acts. Directors' and officers' liability insurance covers losses attributable to negligent acts.

Under 12 CFR § 563.190, Bonds for Directors, Officers, Employees, and Agents; Form of and Amount of Bonds, associations must maintain bond coverage. Coverage must be in an amount that each association determines to be safe and sound in view of the association's potential exposure to risk. In assessing the adequacy of such coverage, management and the board of directors should at a minimum consider the following factors:

- The size of the association's asset portfolio and deposit base.
- An overall assessment of the effectiveness of the association's internal operating controls.
- The amount of cash, securities, and other property that the association normally holds.
- The number of the association's employees, their experience, levels of authority, and turnover rate.

- The extent that the association conducts trust powers.
- The range and scope of information technology activities.
- The extent of coverage that a holding company fidelity bond or other affiliated entity provides.

Paragraph (d) of 12 CFR §563.190 requires the board of directors to review the association's bond coverage at least annually to assess the continuing adequacy of coverage.

During the examination process you are to review the record of management's assumptions, analyses, and conclusions in its determination as to the appropriate form and levels of coverage.

OTS regulations do not require fidelity bond coverage under a specific standardized form. Bond coverage must include each director, officer, employee, and agent who has control over or access to cash, securities, or other property of the association. The board of directors of each association must formally approve the association's coverage, including any endorsements, riders, or other forms of coverage that may supplement the insurance underwriter industry's standard forms.

In addition, an association doing business with a stockbroker must ensure that the stockbroker has Stockbroker's Blanket Bond protection. This protection covers the firm's employees that handle the property of clients. The association should keep a copy of the bond in its files.

For various reasons, such as insufficient levels of regulatory capital, some associations have difficulty in obtaining bond coverage. Supervisory discretion is permissible in these instances when an association documents evidence of its attempts to obtain coverage. The association should notify the regional director of its efforts to obtain such coverage.

An association's periodic review of internal and external logical and physical security measures and controls is appropriate in every association. Refer to [Section 341 of the Examination Handbook](#), and the [Examination Handbook Section on the Bank Protection Act](#). Such review is especially appropriate in an association that is operating without adequate bond coverage. Ideally, an association should undertake this effort as a special project, with responsibility assigned to a particular executive officer. The project should include such matters as the following:

- A thorough review of the association's existing programs.
- The design and implementation of additional security procedures and controls.
- A formal report to the board of directors. The board's minutes should note the board's resulting action.



## D & O Liability Insurance

In addition to fidelity bond coverage, many associations obtain directors' and officers' (D&O) liability insurance. D&O insurance protects directors and officers against personal liability for losses that a third party incurred due to a director or officer's negligent performance.

There is no regulatory requirement that an association maintain D&O insurance. A federal association may self-indemnify directors and officers.

## REFERENCES

### United States Code (29 USC)

§ 201	Fair Labor Standards Act of 1938
§ 206	Equal Pay Act of 1963
§ 621	Age Discrimination in Employment Act of 1967
§ 651	Occupational Safety and Health Act of 1970
§ 1001	Employee Retirement Income Security Act of 1974

### United States Code (42 USC)

§ 2000e	Title VII of the Civil Rights Act of 1964 (Equal Employment Opportunity)
---------	--

### Code of Federal Regulations (12 CFR)

#### *Federal Reserve Board Regulations*

Part 215	Regulation O, Loans to Executive Officers, Directors, and Principal Shareholders of Member Banks
----------	--

#### *OTS Regulations*

§ 528.7	Nondiscrimination in Employment
§ 545.121	Indemnification of Directors Officers and Employees
§ 552.6-2	Officers
§ 561.35	Officer
§ 563.33	Directors, Officers, and Employees

§ 563.39	Employment Contracts
§ 563.41	Loans and Other Transactions with Affiliates and Subsidiaries
§ 563.43	Loans by Savings Associations to Their Executive Officers, Directors and Principal Shareholders
§ 563.161	Management and Financial Policies
§ 563.180	Suspicious Activity Reports and Other Reports and Statements
§ 563.181	Reports of Change in Control of Mutual Savings Associations
§ 563.183	Reports of Change in Chief Executive Officer or Director
§ 563.190	Bonds for Directors, Officers, Employees, and Agents; Form of and Amount of Bonds
§ 563.191	Bonds for Agents
§ 563.200	Conflicts of Interest
§ 563.201	Corporate Opportunity
§ 563.550	Notice of Change of Director or Senior Executive Officer
Part 563f	Management Official Interlocks
§ 565.6	Mandatory and Discretionary Supervisory Actions under Section 38
Part 568	Bank Protection Act
Part 570	Interagency Guidelines Establishing Standards for Safety and Soundness, Appendix A and B

## Office of Thrift Supervision Guidance

### *CEO Memos*

CEO 133	Risk Management of Technology Outsourcing
---------	---

### *Regulatory and Thrift Bulletins*

RB 20	Proper Investigation of Applicants and Increased Communications Between OTS and Other Financial Association Regulatory Agencies
-------	---

RB 27b                      Compensation

TB 81                      Interagency Policy Statement on the Internal Audit Function and Its Outsourcing

TB 82a                      Third Party Arrangements

*Handbook References*

[Section 1100](#)              [Compliance Oversight Examination Program](#)

**This page intentionally left blank**

# Management Assessment Program

---

## EXAMINATION OBJECTIVES

To determine whether management policies, procedures, and strategic plans adequately address safety and soundness, profitability, and compliance with laws and regulations.

To determine whether association officers are operating in conformance with established guidelines, objectives, policies, and procedures.

To determine whether management maintains a comprehensive and effective compliance management program.

To ascertain whether management personnel periodically re-evaluate procedures and practices and implement appropriate modifications, either directly or through recommendations to the board of directors.

To determine whether management plans adequately for future conditions and developments.

To determine whether the association has established policies to ensure an adequate management staff, and has adequate plans for management continuity.

To determine the adequacy of the staff size and expertise for safe operations.

To determine if management adequately controls and supervises the outsourcing of functions and the use of consultants.

## EXAMINATION PROCEDURES

### LEVEL I

WKP. REF.

1. Review previous examination reports, internal and external audit reports, management letters, supervisory correspondence, and any approval conditions. Perform any necessary follow-up procedures to ensure the association took effective corrective action.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Management Assessment Program

---

WKP. REF.

2. Review the following records:
  - Organization chart. Identify key decision-making personnel (include copy in the continuing examination file).
  - Resumes and new employment contracts and executive incentive plans for executive officers and department or division heads. The review should also cover any changes since the last examination.
  - Conflict of interest policy. Determine if the policy ensures regulatory compliance and whether management distributes the policy to directors, officers, and employees.
  - Management's responses to the PERK Management Questionnaire.
  - Details regarding outsourcing arrangements and the use of consultants.

---
3. Determine the extent and effectiveness of management's efforts toward maintaining a comprehensive and reliable internal compliance management program that satisfactorily addresses OTS's SMAART components.

---
4. Determine whether there are any changes in the association's management or directorate and, if applicable, whether the association is in compliance with the notification requirements of 12 CFR §§ 563.550 through 563.590. Notify the regional director if the association is not in compliance.

---
5. Analyze the following types of periodic reports submitted to executive management to determine their usefulness in monitoring the condition and operation of the association:
  - Financial condition reports.
  - Business and strategic plans, budgets, and comparison of performance with budget reports.

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Management Assessment Program

---

WKP. REF.

- Internal audit and loan review reports.
- 

6. Through the review of gathered information, including observations and discussions with management and other personnel, determine the adequacy of the following operational concerns:

- The association's established policies, procedures, and strategic plans that address safety and soundness (including internal controls), profitability, and compliance with laws and regulations.
  - Management's expertise and ability to carry out duties and responsibilities, including corrective actions, in a manner that provides for an acceptable level of safety and soundness, profitability, and compliance with laws and regulations.
  - Management reports and information systems. The reports and systems must provide management and the directors with accurate decision-making information and the ability to monitor compliance with established guidelines.
- 

7. In conjunction with the examiners assigned to the Earnings and Liquidity areas, determine if the association's strategic planning is adequate. Consider the following questions:

- Does the board of directors provide adequate direction?
  - Is the strategic plan realistic based on the association's strengths and weaknesses, and operating environment?
  - Are the assumptions of the plan realistic?
  - Are there sufficient performance measures designed to monitor progress toward specified objectives? Review progress against plan goals.
  - Does the strategic plan include a clear mission statement?
  - Does management effectively communicate the plan throughout the organization?
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Management Assessment Program

---

WKP. REF.

8. Review the fidelity bond and directors' and officers' insurance policies and determine if coverage is adequate.
- 

9. Determine whether management is committed to comply with conditions of approval, orders, supervisory agreements, and directives, if applicable to the association or holding company.
- 

10. Review Level II procedures and perform those necessary to test, support, and present conclusions derived from performance of Level I procedures.
- 

## LEVEL II

1. Complete [General Questionnaire 330, Management Assessment](#).
- 

2. Review and evaluate management compensation to assure that it is adequate and not excessive.
- 

3. Determine whether the association has established any executive incentive plans. If so, determine if such plans could lead to the deterioration of the association's condition or allow beneficiaries of the plan to understate noncash expenses or overstate noncash income. Incentive plans include commissions, referral fees, finder fees, bonus plans, deferred compensation packages, stock option plans, and extravagant fringe benefits.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



# Management Assessment Program

---

WKP. REF.

4. Review the association's activities with regard to developing personnel for senior management succession. At a minimum, this review should include the following considerations:
  - An assessment of the quality of middle and lower levels of management and the potential for advancement.
  - An assessment of the need for and access to developmental training.
  - An assessment of the association's employee screening policies to determine that they are appropriate to protect the safety and soundness of the association.

---
5. When appropriate, interview the personnel manager to determine answers to the following concerns:
  - What personnel policies are currently in effect, and is their application equitable and uniform to all deserving employees?
  - How does the association communicate policies to employees?
  - Are procedures in place to eliminate terminated employees access to assets and records?

---
6. Determine the structure of the association's communication system, both formal and informal, and the extent to which the association adequately informs personnel of strategic goals, policies, and procedures.

---
7. Review records and reports that summarize employee turnover, and interview management personnel and employees. Determine reasons for excessive turnover, if applicable.

---
8. Ask the managing officer or personnel officer if any employees or former employees have brought any discrimination complaints, lawsuits, workers compensation claims,

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Management Assessment Program

---

WKP. REF.

unemployment claims, or wrongful discharge suits against the association during the review period. Compare the responses with the answer in the Management Questionnaire.

---

9. If appropriate, further evaluate management based on your above Level I and II findings and work performed throughout the examination. Consider the following factors:
- The workload of key personnel.
  - The adequacy of the compliance management program and self assessment process.
  - Succession of management and replacement of key personnel.
  - Technical proficiency of officers in their areas.
  - Serious or widespread lack of proper implementation of policies.
  - Deficiencies in the planning process, the strategic plan or its implementation.
  - Promptness with which management recognizes and addresses problems.
  - The extent to which management delegates and demands accountability.
  - Whether management pays more attention to the operations of a functional area rather than with the overall supervision of the association.
  - The degree to which the association is self-regulating, for example, the sufficiency of its systems, such as internal audit and loan review.
  - The appearance of any conflict of interest situations.
  - The overall effectiveness of management based on the association's performance.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Management Assessment Program

---

WKP. REF.

10. Ensure that your review meets the Examination Objectives of this Handbook section. State your findings and conclusions, as well as appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.
- 

## LEVEL III

1. Review written personnel manuals, job descriptions, new employee orientation manuals, and training manuals for employees and supervisors. Determine if manuals and related information are reasonable and in compliance with the provisions of current law and regulations concerning discrimination. Determine whether they include logical and adequate detail with respect to work flows, lines of authority, and areas of job responsibility. Look for any disparate treatment in hiring practices, test requirements, or screening opportunities.

---

  2. Determine whether the institution periodically reviews employee performance, analyzes weaknesses, takes corrective action when appropriate, and has specific policies and procedures for handling employees who have demonstrated incompetence or nonperformance.

---

  3. Review a selected sample of personnel files. Determine whether the association's procedures provide for the systematic updating of personnel files and whether the staff updates in accordance with the schedule. Determine whether the files contain the following information:
    - Payroll deduction authorizations in compliance with state and federal laws.
    - Records of accumulated withholdings.
    - Notations of length of service, salary history, and retirement and other accrued benefits.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Management Assessment Program

---

WKP. REF.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

# Management Assessment

## Questionnaire

---

Yes No

### General Questionnaire

- |    |  |                          |                          |
|----|--|--------------------------|--------------------------|
| 1. | Has the board set overall objectives for management performance and has management met the objectives?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. | Does the association have an organizational chart? If not, have lines of authority and reporting responsibility been formally established?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. | Does senior management receive:  |                          |                          |
|    | • A brief statement of condition daily?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • A daily liquidity report?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • A list of assets subject to internal classification at least monthly?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • A comparative earnings statement, at least monthly?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. | Does management periodically review the association's implementation and maintenance of internal controls (generally through reports that the internal or external auditors provide)? If so, has management determined whether controls: |                          |                          |
|    | • Adequately prevent irregularities by the use of limited authorities, co-approval requirements, and prompt review of transactions for required approvals, as well as propriety?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Adequately deters irregularities by ensuring their timely detection?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Establish and maintain appropriate accountability?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Ensure the maintenance of well-planned records?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Ensure the segregation of duties?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. | Does management maintain a comprehensive and reliable internal compliance management program?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Does the program satisfactorily address OTS's SMAART components?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Does the program include a process of monitoring and assessing compliance performance?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Does management implement corrective action to remedy identified violations or operational deficiencies?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. | Does the auditing function cover officers' compliance with board and management policies?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. | Does the association have policies to ensure the continuity of development and depth of management personnel?  | <input type="checkbox"/> | <input type="checkbox"/> |

**Exam Date:** \_\_\_\_\_

**Prepared By:** \_\_\_\_\_

**Reviewed By:** \_\_\_\_\_

**Docket #:** \_\_\_\_\_

## Management Assessment Questionnaire

	Yes	No
8. Is the staff adequate to facilitate efficient operations?	<input type="checkbox"/>	<input type="checkbox"/>
9. Does the association comply with applicable statutes, regulations, and policy statements?	<input type="checkbox"/>	<input type="checkbox"/>
10. Does the association use a system of written job descriptions and performance standards, including descriptions for supervisory personnel?	<input type="checkbox"/>	<input type="checkbox"/>
11. Does the association perform background investigations on new employees?	<input type="checkbox"/>	<input type="checkbox"/>
12. Does the association have a formal training program?	<input type="checkbox"/>	<input type="checkbox"/>
• Does training include clear communication of relevant legal and regulatory requirements and procedural guidelines, especially those for protecting customer information?	<input type="checkbox"/>	<input type="checkbox"/>
13. Does the association provide management training to those persons likely to assume higher-level positions?	<input type="checkbox"/>	<input type="checkbox"/>
14. When appropriate, do employment termination procedures prevent a terminated employee's ability to control assets and records, access electronic systems, modify or eliminate passwords, change locks, remove signature authorities, and provide proper termination notifications to affected employees?	<input type="checkbox"/>	<input type="checkbox"/>
15. If the association was or is subject to the notification requirement 12 CFR § 563.550 is the association in compliance with the regulation?	<input type="checkbox"/>	<input type="checkbox"/>
16. If the association is subject to the prompt corrective action provisions of OTS regulation § 565.6(a), is it in compliance with the management fee and executive officer compensation restrictions of FDIA § 38?	<input type="checkbox"/>	<input type="checkbox"/>
17. Do the association's executive compensation and employment contracts comply with 12 CFR § 563.39, § 563.161, and OTS policy set forth in Regulatory Bulletin 27b?	<input type="checkbox"/>	<input type="checkbox"/>
18. Are the quality, quantity, and timeliness of the association's management information systems adequate?	<input type="checkbox"/>	<input type="checkbox"/>
19. Is management responsive, in a timely manner, to supervisory criticism?	<input type="checkbox"/>	<input type="checkbox"/>
20. Is the association in compliance with the restrictions of OTS regulation § 563.43, concerning loans to officers, directors, and principal shareholders?	<input type="checkbox"/>	<input type="checkbox"/>
21. Are management's assumptions, analyses, and conclusions regarding the appropriate fidelity bond form and level of coverage reasonable and acceptable?	<input type="checkbox"/>	<input type="checkbox"/>

**Exam Date:** \_\_\_\_\_  
**Prepared By:** \_\_\_\_\_  
**Reviewed By:** \_\_\_\_\_  
**Docket #:** \_\_\_\_\_



**This page intentionally left blank**



## Internal Control

OTS requires all savings associations, their affiliates, and subsidiaries to establish and maintain adequate systems of internal control. As financial institutions reposition their portfolios, they must have a process in place to identify, monitor, and control risk. Audits by public accountants and examinations by all the banking agencies have placed a greater emphasis on evaluating the appropriateness of the processes in place, and less reliance on transaction testing.

The Auditing Standards Board (ASB) revised its definition of internal control in Statement of Auditing Standard (SAS) No.78, Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55, Consideration of Internal Control in a Financial Statement Audit. The revised definition incorporates the common critical elements of internal control systems in Committee of Sponsoring Organizations of the Treadway Commission (COSO) report, issued in 1992.

---

### L I N K S

<hr/> <a href="#">Program</a>	This section of the Handbook defines internal control, describes objectives and components of internal control, and explains how to consider internal control in planning and performing an examination. In general, when beginning an examination, first review and evaluate the adequacy and effectiveness of the internal control system. If you discover areas where internal controls are inadequate, expand the scope of examination to determine whether there are any safety and soundness concerns.
<hr/> <a href="#">Appendix A</a>	

## OBJECTIVES

An effective internal control system better ensures the following important attributes:

- Safe and sound operations.
- The integrity of records and financial statements.
- Compliance with laws and regulations.
- A decreased risk of unexpected losses.
- A decreased risk of damage to the association's reputation.
- Adherence to internal policies and procedures.

- Efficient operations.

A system of strong internal control is the backbone of an association's management program. Strong internal control helps an association to meet goals and objectives, and to maintain successful, healthy operations. Conversely, a lack of reliable records and accurate financial information may hamper the long-term viability of an association. An effective internal control system integrated into the organization's overall risk management strategy serves the best interest of the shareholders, board of directors, management, and regulators.

## REGULATORY CONCERNS

Regulators are placing increasing importance on internal control systems in light of recent financial association failures. Some associations failed primarily because they did not detect insider fraud or abuse because they had deficient or nonexistent systems of internal control. The Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991 required the banking agencies to establish certain safety and soundness guidelines. Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness, includes a section on operational and managerial standards.

Under these standards, OTS requires management and the board of directors to implement and support effective internal controls appropriate to the size of the association, its nature, and scope of activities.

## DIRECTORATE RESPONSIBILITIES

The board of directors has the primary responsibility of establishing and maintaining an adequate and effective system of internal control. An effective board generally has members who have financial or banking experience, and stature.

The board is responsible to report to the FDIC and the OTS (when it is the primary regulator) on internal control over financial reporting and compliance with certain laws and regulations, as well as filing annual audited statements under Section 112 of FDICIA.

The board is also responsible for approving and periodically reviewing the overall business strategy and significant policies of the association, as well as understanding the major risks the association takes. The board should set acceptable levels for these risks, and ensure that senior management takes the required steps to identify, measure, monitor, and control these risks. To remain effective in the dynamic and ever broadening environment that associations operate in, the board of directors should periodically review and update the internal control system.

To oversee internal control and the external and internal audit function of an association, an audit committee comprised of outside directors (or at least a majority of outside directors) is desirable. Insured depository institutions covered by Section 36 of the Federal Deposit Insurance Act (assets total

\$500 million or more), as implemented by 12 CFR § 363.1(a) must have an audit committee composed of only outside directors.

An active board or audit committee independent from management sets the association's control consciousness. The following parameters determine effectiveness:

- The extent of its involvement in and its scrutiny of the association's activities.
- The ability to take appropriate actions.
- The degree to which the board or audit committee asks difficult questions and pursues the answers with management.

For additional guidance on audit committee responsibilities, see Handbook Section 355, Internal Audit.

## AUDITOR RESPONSIBILITIES

### Internal Audits

Both the internal and external auditors play key roles in the monitoring of internal control systems. Each association should have an internal audit function that is appropriate to its size, and the nature and scope of its activities. The internal auditor is typically very involved in the ongoing review and assessment of an association's internal control. The board of directors should assign responsibility for the internal audit function to a member of management who has no operating responsibilities, and who is accountable for audit plans, programs, and reports. When properly structured and conducted, internal audits provide directors and senior management with vital information about any weaknesses in the system of internal control allowing management to take prompt, remedial action. Through directed reviews of the internal control systems and as part of the regular audit program, the internal auditor can be the first line of defense against a corrupted control system.

### External Audits

Established policies and practices look to the external auditor to play a significant and vital role in an association's internal control systems. In this role, the external auditor performs examination procedures to attest to management's assertion that the internal control over financial reporting is functioning effectively, and that it is in compliance with designated laws and regulations. The external auditor may consider the work done by the internal auditor as part of the auditing procedures.

SAS No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control*, which amends SAS No. 55, provides guidance to auditors about the effect of information technology on internal control. It also establishes that an auditor should obtain an understanding of internal control sufficient to plan the audit and determine the nature, timing, and extent of tests to perform, including assessment of control risk. While this pronouncement places significant responsibility on the external auditor to look at internal control, the external auditor may not extensively review controls over all areas of the association, and may use different levels of testing depending on the risk of a specific area.

SAS No. 60, *Communication of Internal Control Related Matters Noted in an Audit*, provides guidance to the external auditor in identifying and reporting conditions that relate to an association's internal controls observed during an audit of financial statements. The reportable conditions discussed in this pronouncement are matters coming to the attention of the auditor that, in the auditor's judgment, should be communicated to the audit committee because the conditions represent significant deficiencies in the design or operation of internal control. These conditions, in the opinion of the auditor, could adversely affect the association's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. In some instances, a reportable condition may be of such magnitude to be a "material weakness." A material weakness in internal control is a reportable condition in which the design or operation of one or more of the internal control components does not sufficiently reduce the level of risk that material misstatements caused by error or fraud may occur, and employees in the normal course of business would not timely detect the misstatements.

Auditors generally do not search for reportable conditions or material weaknesses. They usually become aware of them through consideration of the components of internal control, application of audit procedures to balances and transactions, or during the course of the audit. The auditor makes a judgment as to which matters are reportable, taking into consideration various factors, such as an entity's size, complexity and diversity of activities, organizational structure, and ownership characteristics.

When examining the communication of internal control matters noted in an audit, be aware that there is no standard form of communicating reportable conditions or material weaknesses to the audit committee. Once the auditor has chosen to discuss reportable conditions or material weaknesses, the auditor may do so either through a formal presentation to the audit committee, or informally, through conversations. The auditor may also submit written reports. Generally, the auditor will document oral communications by appropriate memoranda or notations in the working papers.

## INTERNAL CONTROL COMPONENTS

SAS No. 78 provides guidance on the independent auditor's consideration of an entity's internal control in an audit of financial statements in accordance with generally accepted accounting standards. SAS No. 78 recognizes the definition and description of internal control contained in the COSO report, and provides an overview of the framework and evaluation tools needed for a strong system of internal control. OTS urges association management and boards of directors to consider SAS No. 78, or other recognized standards in developing and maintaining an effective system of internal control.

SAS No. 78 consists of five interrelated components derived from the way management runs a business, and integrated with the management process. The components are:

- Control environment
- Risk assessment
- Control activities

- Information and communication
- Monitoring.

### The Control Environment

The effectiveness of internal controls rests with the people of the organization who create, administer, and monitor them. Integrity and ethical values are essential elements of a sound foundation for all other components of internal control. The commitment for effective control environment rests at the top. Reaching a conclusion about a financial institution's internal control environment involves a degree of subjectivity because of the intangible nature of measuring effectiveness.

#### *Control Environment Assessment Process*

Draw conclusions as to the quality of risk management and assess the effectiveness of the control environment in the following areas:

#### Integrity and Ethical Values

Integrity and ethical values are the products of the association's ethical and behavioral standards. How management communicates and reinforces these values in practice establishes the "tone" for the organization. Management should strive to remove or reduce incentives and temptations that might prompt employees to engage in dishonest, illegal, or unethical acts. Management must also communicate their values and behavioral standards to personnel through policy statements and codes of conduct.

#### Management Philosophy and Operating Style

Management's approach to taking business risks and their attitude toward financial reporting (conservative versus aggressive) and information processing weigh heavily in the control environment. Consider the level of commitment by management and the board of directors to establish the necessary foundation on which to build an effective system of internal control. Management must have the will to make policies work or even the best-written policies on internal control lose effectiveness.

#### Organizational Structure

The association must have an organizational structure that supports its objectives. Management must plan, execute, control, and monitor association objectives. It must establish key areas of authority and responsibility and appropriate lines of reporting.

#### Assignment of Authority

Assignment of authority includes policies relating to the following areas:

- Appropriate business practices.

- Knowledge and experience of key personnel.
- Resources for carrying out duties.

#### Human Resource Policies and Practices

Human resource practices send messages to employees regarding expected levels of integrity, ethical behavior, competence, and conflict of interests.

#### Risk Assessment

All entities, regardless of size, encounter risk in their organizations. The ability to identify and manage these risks will affect an entity's ability to survive in a competitive market. In order to assess risk, management must first set objectives to quantify the amount of risk they can prudently accept.

Risks relevant to financial reporting include external and internal events, and circumstances that may adversely affect an association's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. Such risks can arise or change due to the following circumstances:

- Operating environment changes
- New personnel
- New or revamped information systems
- Rapid growth
- New technology
- New lines, products, or activities
- Corporate restructuring
- Accounting pronouncements.

#### *The Risk Assessment Process*

Determine whether management has identified and analyzed the risks, and has methodologies in place to control them. Consider also the following areas in assessing the risk process:

- Prevalence of external and internal factors that could affect whether strategic objectives are achieved.
- Effectiveness of systems used to manage and monitor the risks.

- Capacity of existing processes to react and respond to changing risk conditions.
- Level of competency, knowledge, and skills of personnel responsible for risk assessment.

### Control Activities

Control activities are the policies and procedures that help ensure management carries out its directives. Control activities should assure accountability in the association's operations, financial reporting, and compliance areas.

#### *The Control Activities Assessment Process*

Assessment of control activities relevant to an examination includes the elements discussed below.

#### Performance Reviews

Management should establish policies and procedures to ensure control activities include reviews of actual performance versus budgets, forecasts, and prior period performance.

Management should conduct independent checks or verifications on function performance and reconciliation of balances.

#### Information Processing

There are two broad groupings of information systems: General controls and Application controls.

Management should establish policies and procedures to ensure that general controls are commonly in place over the following areas:

- Data center operations.
- System software acquisition and maintenance.
- Security access.
- Application system development and maintenance.

Management should also establish policies and procedures for application controls, which apply to the processing of individual applications. These controls ensure valid, complete, properly authorized, and accurately processed actions.

#### Physical Controls

Management should establish safeguards and physical controls over the following activities:

- The physical security of assets, such as secured facilities.

- Access to books, and sensitive records and systems.
- Authorization for access to computer programs and data files.

### Segregation of Duties

Management should reduce the opportunities to perpetrate and conceal errors, irregularities, or any wrongdoing. Management must assign different people the responsibility of authorizing transactions, recording transactions, and maintaining custody of assets. For these safeguards, management should ensure that vacation requirements or periodic rotation of duties for personnel in sensitive positions occurs.

### Information and Communication Systems

Management must identify, capture, and communicate information to enable people to carry out their responsibilities. Internally generated data, along with external events, activities, and conditions is necessary for a business to make informed decisions.

To be effective, management must communicate information to the people who need it to carry out their responsibilities. Management must design ways to downstream messages from the top, as well as upstream significant information.

An information system should provide sufficient detail to properly classify the transaction for financial reporting, and measure the value of the transactions in a manner that permits recording the proper monetary value in the financial statements in accordance with GAAP.

### *Information and Communication Systems Assessment Process*

Communication involves an understanding of individual roles and responsibilities pertaining to internal control over financial reporting. Determine whether policy manuals, accounting and financial reporting manuals, and other memoranda effectively communicate internal control responsibilities.

Determine if management established systems to capture and impart pertinent and timely information in a form that enables staff to carry out their responsibilities. Also, determine whether the following safeguards exist:

- Accounting systems identify and record all valid transactions in the proper accounting period, ensure accountability for related assets and liabilities, and present transactions and related disclosures in the financial statements.
- Management information systems identify and capture relevant internal and external information in a timely manner.
- Contingency plans exist for information systems.



## Monitoring

Monitoring is a process that assesses the quality of the internal control performance over time. Management must build ongoing monitoring activities into the normal recurring activities of their association, and monitor the internal control system on an ongoing basis to ensure that the system continues to be relevant and addresses new risks. In many cases, the internal auditor is responsible for monitoring the entity's activities and regularly provides information about the functioning of internal control, including the design and operation.

### *The Monitoring Assessment Process*

Determine who oversees and assesses the monitoring process. Review the type of periodic evaluation of internal control that occurs. For example, is it by self-assessment or by independent audit? Check whether systems ensure timely and accurate reporting of deficiencies and whether there are processes to ensure timely modification of policies and procedures, as needed.

## ASSESSING CONTROL RISK

Under SAS No. 78, control risk is the risk that the entity's internal control system will not prevent or detect on a timely basis a material misstatement. Assessing control risk is the process of evaluating the design and operating effectiveness of an entity's internal control. Although you do not ordinarily consider the individual components of internal control, you should consider the combined aspects of the five SAS No. 78 components.

- You can assess control risk in quantitative terms, such as percentages, or in nonquantitative terms that range from maximum to minimum.

### Assessing Control Risk at the Maximum

You should assess control risk at the maximum when there is risk that internal control will not prevent or detect material misstatements on a timely basis. In addition, you should review control risk at the maximum if management's representations conflict with controls or reduce the effectiveness, or you have concern that you cannot obtain sufficient competent evidential matter to evaluate the effectiveness of internal controls.

### Assessing Control Risk at Less Than Maximum

Assessing control risk below the maximum involves performing tests to evaluate the effectiveness of such internal control. Tests of controls should determine whether the control is suitably designed to prevent or detect material misstatements. These tests ordinarily include evidence obtained from the following actions:

- Conducting management inquiries.
- Inspecting documents and reports to review how staff performs controls.

- Observing directly how management applies the controls.
- Retesting how management applies the controls.
- Evaluating if management designs an effective internal control system to monitor and correct noncompliance.
- After examining the components and their risk, draw an overall conclusion as to the adequacy of the association's system of internal control and include the assessment in the report of examination. A system deemed inadequate is potentially in noncompliance with Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness. OTS may notify an association with an inadequate assessment of the need to file a plan of compliance as provided for under the regulations. The plan would establish the manner in which the association will rectify its internal control deficiencies.

## Overall Assessment

The overall risk assessment should determine whether management takes the following actions:

- Supports fully the concept of effective internal control.
- Encourages their employees to comply with the controls.

## LIMITATIONS OF INTERNAL CONTROL

When operating under the best of conditions, internal control provides only reasonable assurance to management and the board of directors that the association is achieving its objectives. Reasonable assurances do not imply that the internal control systems will never fail. Many factors, individually and collectively, serve to provide strength to the concept of reasonable assurance. However, because of inherent limitations, management has no guarantee that, for example, an uncontrollable event, a mistake, or improper reporting incident could never occur. Thus, it is possible for the best internal control system to fail. The limitations inherent to internal control are:

- Judgment
- Breakdowns
- Management override
- Collusion
- Fraud
- Cost versus benefits.

We discuss each of these limitations below.

### Judgment

Human judgment can limit the effectiveness of internal controls. Management makes business decisions based on the information at hand and under time constraints. With hindsight, these decisions may produce less than desirable results.

### Breakdowns

The best internal control system can experience any of the following breakdowns:

- Misunderstood instructions
- Careless employees
- Inadequate training
- Time limitations.

### Management Override

Management override means management overrules prescribed policies or procedures for illegitimate purposes with the intent of personal gain or to enhance the presentation of financial statements. Override practices include deliberate misrepresentations to regulators, lawyers, accountants, and vendors.

Do not confuse management override with management intervention. Management intervention represents management's actions that depart from prescribed policies for legitimate purposes. At times, management intervention is necessary to deal with nonrecurring and nonstandard transactions or events, that otherwise might be handled inappropriately by the control system.

### Collusion

When two or more individuals act in concert to perpetrate and conceal an action from detection, they can circumvent any system of internal control.

### Fraud

Fraud is a broad legal concept, and involves intentional illegal acts that generally cause misstatement in the financial statements. Management bears the primary responsibility for detecting fraud. Internal control systems implementation is part of management's fiduciary responsibilities to prevent fraud and abuse by insiders. While the primary objective of an examination is the qualitative analysis of the association, fraud detection is certainly a goal when reviewing an association's internal control system.

Recent problems concerning insiders at some associations have some commonalities. Potential red flags that could signal fraud include the following situations:

- Management that is hostile or uncooperative towards examiners.
- Significant insider transactions that the association improperly approves or fails to fully document.
- Basic internal control deficiencies, such as failure to separate functions or rotate duties.
- Poor or incomplete documentation.
- Financial accounting systems and reports are unreliable, underlying controls are deficient, or the reconciliation process is lacking.
- Repeated and significant Thrift Financial Report reporting errors.
- Continuing unsafe and unsound conditions.

You should be aware of the potential warning signs of fraud and the examination and audit procedures that you should employ when warranted. If you encounter any red flags, you should bring the situation to the attention of the Regional Accountant. For more information, see [Examination Handbook Section 360, Fraud and Insider Abuse](#).

## Costs versus Benefits

The challenge is to find the right balance between the proper controls and the costs to design and implement internal controls. Excessive control is costly and counterproductive. Too few controls present undue risks.

## EXAMINATION APPLICATIONS

### Internal Control and Funds Transfer Questionnaires

The objective of examining the internal control of an association is to assess the extent to which management has established internal control procedures and programs to identify and mitigate the association's internal control risks. In planning the examination, be aware of the following situations that may suggest that there is a breach in the control system that warrants attention:

- Management does not implement effective procedures to correct internal deficiencies noted in audit reports.
- Management scales back or suspends the internal audit function.

- The internal auditor has an operational role in addition to audit responsibilities. For example, the internal auditor reports through operating management and not directly to the board of directors or a committee. Ideally, the internal audit function should be under the board of directors or the audit committee, and the internal auditor should report directly to them. The extent to which the internal auditor reports to management may warrant attention to ensure that such reporting does not impair the independence of the internal auditor.
- The association's external audit firm lacks savings association or bank audit experience, or the auditors assigned have limited experience.
- The association enters new areas of activity without first implementing proper controls, or engages in new activities without experienced staff and appropriate controls in place.
- The association fails to provide adequate reports to the board of directors.
- The association does not have proper controls in high-risk areas.
- The association often deviates from board-approved policies with exception documentation.
- The association fails to effectively segregate duties and responsibilities among employees.

### *Level I Procedures*

Review the list of objectives in the Internal Control Program, included in the Appendix of this Handbook section, and follow the Level I Procedures to design the examination. These procedures are generally sufficient when an association has an effective internal audit function.

Although the five components of internal control provide a useful framework for you to review the effect of an entity's internal control in an examination, they do not reflect how the association considers and implements internal control. Therefore, you should consider the five SAS No. 78 components in the context of the following criteria:

- Size of the association.
- Organization and ownership characteristics.
- Nature of the association's business.
- Diversity and complexity of the association's business.
- Methods of transmitting, processing, maintaining, and accessing information.
- Legal and regulatory requirements.

### *Management's Responses*

OTS sends questionnaires to the association as part of the PERK. Association management answers the Internal Control Questionnaire and the Funds Transfer Questionnaire, which contain questions regarding the overall internal control system of the thrift. You should verify answers provided by management to ensure that the answers accurately reflect the association's activities.

In both the [Internal Control and Funds Transfer Questionnaires](#), there are certain "flagged" questions that are the minimum verifications you should perform.

### *Internal Audit Work Papers*

Examine samples of work papers from internal audits, and include samples from outsourced functions or director's examinations. The samples should be sufficient to provide a basis to validate the scope and quality of the association's internal control system, and determine the amount of reliance, if any, you can place on the system.

Review also, whether the external auditor communicated any reportable conditions, either orally or in writing, to management. If you determine that external audit work papers are necessary for your review, contact the Regional Accountant before requesting external audit work papers, or other pertinent documents related to the external auditor's judgment about the association's internal control. See [Handbook Section 350 for requesting external audit work papers, Appendices D and E](#).

Make requests for work papers specific to the areas of greatest interest. The request may include related planning documents and other pertinent information related to the internal control areas in question. If management or the internal auditor refuses to provide access to the work papers, contact the Regional Accountant.

If the internal audit work papers review or the external auditor's communications with management on reportable conditions raises concerns about audit effectiveness, discuss the issues with management, the board of directors, and the audit committee. If issues remain unresolved regarding external audit work, consult the Regional Accountant.

### *Level II Procedures*

Based on management's responses to questionnaires, or when an association does not have an effective system of internal audit, or when warranted based on examination findings, consider expanding the scope of the examination to include Level II procedures provided in the Internal Control Program. Also perform appropriate Level II procedures if the association outsources any significant activities and Level I procedures are insufficient to determine how the association controls the outsourced activity.

Issues that would require expanded procedures under Level II include:

- Concern about the competency or independence of internal auditors.
- No internal audit program is in place.

- Unexplained or unexpected changes occurring in the internal or external auditors, or significant changes occurring in the audit program.
- Inadequate controls in key risk areas.
- Deficient audit work papers in key risk areas, or work papers that do not support audit conclusions.
- High growth areas exist without adequate audit or internal control.
- Inappropriate actions by insiders to influence the findings and scope of audits.

If significant concerns remain about the adequacy of internal control, the next step, after completion of Level II procedures, should be to consider expanding the scope of the review to include procedures under Level III of the Internal Control Program. The following situations may warrant Level III procedures:

- Account records are significantly out of balance.
- Management is uncooperative or poorly manages the thrift.
- Management restricts access to records.
- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
- Internal auditors are unaware of, or unable to sufficiently explain, significant deficiencies.
- Management engages in activities that raise questions about its integrity.
- Repeated violations of law affect audit, internal control, or regulatory reports.
- Other situations that you believe warrant further investigation.

Consult with the Regional Accountant to determine which procedures you should perform.

## OUTSOURCING RISKS

Associations rely increasingly on services provided by third parties to support a wide range of activities. Outsourcing, both to affiliated companies or third parties, may help manage costs, improve and expand services offered, and obtain expertise not internally available. At the same time, reduced operational control over outsourced activities may expose an association to additional risks.

Outsourcing involves some of the same operational risks that arise when an association performs a function internally. Such risks include the following:

- Threats to the availability of systems used to support customer transactions.
- The integrity or security of customer account information.
- The integrity of risk management information systems.

Under outsourcing arrangements, however, the risk management measures commonly used to address these risks, such as internal controls, are generally under the direct control of the service provider, rather than the association that bears the risk of financial loss, damage to its reputation, or other adverse consequences.

OTS expects associations to ensure that controls over outsourced activities are equivalent to those that the association would implement if they conducted the activity internally. The association's board of directors and senior management should understand the key risks associated with the use of service providers. They should ensure that an appropriate oversight program is in place to monitor each service provider's controls, condition, and performance. See discussion of outsourcing in [Handbook Section 355, Internal Audit](#).

## REFERENCES

### United States Code (12 USC)

#### *Federal Deposit Insurance Act*

§ 1831                      Contracts Between Depository Institutions and Persons Providing Goods, Products, or Services

§ 1831p-1                  Standards for Safety and Soundness

### Code of Federal Regulations (12 CFR)

Part 363                    Requirements For External Audits And Audit Committees

Part 570                    Appendix A, Interagency Guidelines Establishing Standards for Safety and Soundness

## OTS References

Directors' Guide to Management Reports

<http://www.ots.treas.gov/docs/48091.pdf>



## AICPA Professional Standards

### *Statement of Auditing Standards (U.S. Auditing Standards (AU))*

- |        |   |
|--------|---|
| No. 55 | Consideration of Internal Control in Financial Statement Audit (AU 319)   |
| No. 60 | Communication of Internal Control Structure Related Matters Noted in an Audit (AU 325)  |
| No. 78 | Consideration of Internal Control in a Financial Statement Audit: An Amendment SAS 55 (AU 319)                                  |
| No. 94 | The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit (AU 319) |

**This page intentionally left blank**

# Internal Control Program

---

## EXAMINATION OBJECTIVES

Determine whether existing controls reasonably ensure all of the following:

- Accurate and reliable accounts and records.
- Properly authorized transactions.
- Adequately safeguarded assets.
- Compliance with applicable laws and regulations.
- Identification of weaknesses that require further examination (testing) and correction.

## EXAMINATION PROCEDURES

Perform the procedures that summarize the internal controls review. The procedures require the input of other regulators on the team.

### LEVEL I

WKP. REF.

Level I procedures are typically sufficient when an association has an effective internal audit function in place and no findings develop that would cause an expansion of scope.

1. In consultation with the examiner in charge (EIC), review and evaluate the responses to the Management Questionnaire (PERK 002), the Internal Control Questionnaire (PERK 004), and the Funds Transfer Questionnaire (PERK 018). Follow up by reviewing appropriate internal audit work papers and by interviewing the internal auditors and operations staff to determine possible areas of internal control weaknesses. Perform this review as early in the examination as possible. Immediately notify the examiner assigned any area where there are possible weaknesses so the examiner can make any necessary scope changes.
- 
2. Review management reports on internal controls and related attestations by independent accountants required by the Federal Deposit Insurance Corporation Improvement Act (FDICIA). Review the external audit internal control work papers or other communications regarding reportable conditions.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Control Program

---

WKP. REF.

3. Check for material weaknesses in internal controls by noting any deficiencies reported in the following:

- Recent internal and external audit reports.
- Related management letters.
- Management and the board of directors' responses.
- The most recent examination reports of all types.

Determine if management has corrected the deficiencies. Determine the reasons if management has not taken effective corrective action. If management has not taken effective corrective action or if new deficiencies developed, follow appropriate procedures for reporting.

---

4. Determine whether management modified its program of internal control through policy or procedural changes since previous examinations of all types. If so, evaluate the reasons for, and the validity of, such changes.

---

5. Determine whether management established an effective system of internal control and enforces the controls for subordinate organizations and other subsidiaries.

---

6. Verify that management enforces all critical policies.

---

7. Review the general questionnaires as other examiners complete them during the examination to identify all critical internal control weaknesses noted. Discuss these weaknesses with appropriate management personnel, either personally or by the examiner responsible for the review of these areas.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Control Program

---

WKP. REF.

8. Verify that appropriate staff performs reconciliation of general ledger accounts with subsidiary ledgers, supporting documentation, or external confirmations often. Check whether the association promptly clears or resolves reconciling items. (You may do these verifications piecemeal as part of several other examination programs.)  

---
9. Determine whether the association outsources any significant activities to third-party vendors. Review internal and external audit reports for identified problems or concerns regarding outsourced activity. Perform Level II procedures as appropriate.  

---
10. If the association uses its external auditors to conduct the internal audit, determine that the association maintains the integrity and quality of internal control.  

---
11. Determine the presence and effectiveness of internal control activities in all major business lines.  

---

## LEVEL II

You should perform Level II procedures when an association does not have an effective system of internal audit or when warranted based on examination findings. You should also perform appropriate Level II procedures if the association outsources any significant activities and Level I procedures are insufficient to determine how the association handles and controls the outsourced activity.

1. Determine whether the external auditor appropriately evaluated internal control by reviewing the engagement letter and management letter on internal controls. Review audit work papers only after consulting with the EIC and/or the FM.  

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Control Program

---

WKP. REF.

2. Determine whether internal audit or alternate control reviews are sufficiently independent. Pay particular attention to independence issues when the association uses the external auditors to conduct the internal audit.
- 

3. Determine the frequency of testing and reporting for compliance with laws and regulations. Determine whether the association gives appropriate attention and follow-up to violations of laws and regulations.
- 

4. Assess the adequacy of information and communication systems.
- 

5. Determine whether management gives appropriate and timely attention to material control weaknesses once identified.
- 

6. Review outsourcing contracts with third-party vendors to determine their existence and that they are sufficiently detailed commensurate with the scope and nature of the outsourced activity. (See the discussion of [Outsourcing in Handbook Section 355](#).)
- 

7. Determine that the third-party vendor has implemented internal control policies and procedures comparable to those that the association would utilize if the association conducted the activity internally.
- 

8. Determine that the association properly documents and approves all insider and affiliated party transactions.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Control Program

---

WKP. REF.

9. Review director's, officer's, and employee's deposit accounts for any unusual activity.

- 
10. Ensure that your review meets the Objectives of this Handbook Section. State your findings and conclusions as well as appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.
- 

## LEVEL III

After consultation with the field manager you should perform agreed upon Level III procedures based on findings from Level I and Level II procedures. You should also consider Level III procedures when:

- Level I and II procedures are insufficient to draw sound conclusions.
  - The association is not audited by an independent party.
  - The association does not have an internal audit program in place.
1. Verify cash on hand. Review cash items or any other assets or liabilities held in suspense accounts to determine proper and timely disposition.

- 
2. When control concerns exist in a given area or activity, prove subsidiary records for targeted area to the general ledger such as loans, investments, or deposits.
- 

3. Verify the safekeeping of securities on hand or held by others.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Control Program

---

WKP. REF.

4. Review accrued interest accounts and test the computation and disposition of interest income.

---

5. Verify the loan balances for loans charged-off since the previous examination and the debit entries to the allowance account.

---

6. Check supporting documentation for loans charged-off.

---

7. Review loan recoveries and check the credit entries in the allowance account.

---

8. Review closed deposit accounts to determine that they were properly closed. Review dormant account activity for propriety.

---

9. Review deposit overdraft activity to determine legitimacy and adherence to policies.

---

10. Review the timeliness and adequacy of all bank account reconciliations.

---

11. Review all suspense accounts and ascertain explanations for large or unusual items. Determine that no one is using a suspense account to divert deposits, conceal impaired or worthless assets, or hide shortages.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



# Internal Control Program

---

WKP. REF.

12. With the written concurrence of the field manager, conduct a direct verification of appropriate loan or deposit accounts.

---

13. Review the timeliness of wire transfer verifications and reconciliations and verify that independent parties were involved in the process.

---

14. Determine that association management properly supports and approves entries to the books and records and that they review unusual entries.

---

15. Request documentation for significant or unusual transactions. Review the tax return for disclosures.

---

## EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

**This page intentionally left blank**

This discussion briefly addresses subjects in the Internal Control Questionnaire and Funds Transfer Questionnaire. The association completes these Questionnaires as part of the PERK. You should follow up with an interview and indicate on the form any answers that you verified. The association must explain negative responses and you should review through interview and observation any problems needing supervisory attention. Many of these topics are somewhat self-evident and the Handbook covers others in more detail in other sections.

## Internal Control Questionnaire

### *Internal Audit*

Associations should have an internal auditing program that is appropriate to its size and the nature and scope of its activities. Associations should follow specific procedures to test accounting information and internal routine and controls. Preferably, the internal auditor should report findings to the board of directors or an audit committee consisting of outside directors. Internal audit reports should include suggested corrective actions to noted problems. The board or audit committee should ascertain whether management made adequate corrections when recommended. A full-time internal auditor should preferably serve the board or audit committee. If this is impractical, at least the board or audit committee should review the auditor's performance. It should set the salary to keep the auditor independent of the audit subjects, especially top management. Refer to [Examination Handbook Section 355, Internal Audit](#).

### *General Items*

The records and systems should enable others to trace any given item as it passes through the association's books. Exception or large item reports list all transactions over a specific dollar amount, regardless of whether they involve cash, check, etc. The association should have a person not involved in the transaction review the report for unusual items. You may suggest to management that they create such reports if the association does not currently prepare them.

### *Cash and Cash Items*

Cash items are "near cash" checks received as deposits from customers. In the normal course of business, the association sends these items to a correspondent that collects them from the drawee institution. The association receives immediate credit for them. The correspondent will return some items as cash items in which the association will have to resend for collection again. The association may also return them to the depositor.

Checks drawn on uncollected funds in an association are a form of loans to depositors. Management should use software controls and a daily drawing on uncollected funds report to monitor these checks. You can identify these checks by deposit accounts with deposit totals for the past three days being greater than the balance for the day. Checks drawn on uncollected funds must be limited to prevent abuse by depositors unworthy of credit. Some associations reject all checks drawn on uncollected funds. If an association permits drawings on uncollected funds, then management should allow such drawings only after they make a credit decision on the creditworthiness of the depositor. You should determine how management controls or prevents checks drawn on uncollected funds.

Overdrafts are loans made by paying checks that draw a deposit account into a negative (debit) balance. Management should permit overdrafts only after it makes a credit decision on the customer (borrower). An officer should review overdraft activity every day for old, overly large, or inappropriate overdrafts.

Return items are checks deposited in an association, but drawn elsewhere and returned for some reason, usually non-sufficient funds (NSF). The normal procedure for handling return items is to call the depositor and ask if the depositor knows if the item will be good if sent for collection on that day, or if it should be bought back by the depositor. The appropriate staff person should record return items as return item assets if not debited to a customer's deposit account. The association should not hold return items for days pending a decision. They may result in losses, if not paid soon. Management should maintain over and short accounts for each person with a cash drawer. If activity is minimal, then each entry should identify the person with the cash difference. Larger operations may have over and short accruals to compare actual performance with projections.

Management must ensure that accounting controls over all liquid assets prevent personal use by employees. Management's policies should not permit "IOUs" in cash or cash item totals. An appropriate staff person should record all cash and cash item transactions and review them daily to limit abuse.

### *Association (Official) Checks*

Many associations use checks drawn on themselves (known variously as "on-us checks" or "official checks") for payment of expenses, interest, dividends, and loan proceeds. They may also sell them to customers as cashier's checks or money orders. The association must honor its own checks or risk its reputation. The association cannot reject its checks unless there is fraud. For these reasons, management must have policies in effect to control official checks.

One common control is to require two authorized signatures. If management does not require two signatures, someone without signature authority should control the unsigned blank checks. This person should fill out the check amount and payee based on an approved voucher. The approving officer should compare the voucher to the check before signing it. Ideally, the appropriate staff person should verify unused check supplies to a shipping invoice to ascertain that the supply has not been lost and subject to misuse. After checks are paid, someone should review the checks for authorized signatures and compare them with vouchers for alteration. Someone should reconcile copies of outstanding checks to vouchers and the respective liability accounts.

### *Due From Banks*

Due from banks describes assets that consist of demand and time deposits maintained in other financial institutions to facilitate the transfer of funds. Also called correspondent bank balances, these accounts enable the transfer of funds between financial institutions, resulting from the collection of cash items and cash letters, the transfer and settlement of securities transactions, the transfer of participating loan funds, the purchase or sale of federal funds, and from many other causes. Shortcomings in procedures and controls, as they relate to due from bank accounts, can lead to manipulation and shortages. The association must check incoming statements from banks to record copies in each instance to protect against fraud and errors.

*Investments and Securities*

Transactions in investment securities are typically large and involve liquid movable assets, thus making controls in this area very important. To ensure accurate records as well as discourage fraud, appropriate staff should implement the following controls:

- Document transactions and maintain them separately from the initiating officers and the executing traders (if the association has its own trading operation).
- Record all transactions and all holdings in a securities ledger system.
- Reconcile the transactions and the securities ledger to confirmations and broker statements daily.
- Reconcile transactions and the securities ledger to the general ledger at least monthly.
- Maintain accrual accounts to ensure income is collected.
- Review broker statements and confirmations and reconcile them to the books before they go to the investment officers (this action limits the chance of abuse by unauthorized officers in concert with brokers).

Management should enforce policies that limit, by dollar amount, board-granted investment authorities. They should require dual approval for unusually large transactions. Management should make this policy clear to brokers doing business with the association. Brokers should never have the authority to manipulate association assets without prior approval for every transaction. Investment advisors should advise the association, not the broker.

Brokers frequently engage in borrowing of customers' assets through repurchase agreements or use of customers' assets as collateral for their own trading. Management should only permit this for the most creditworthy dealers, who are typically the primary dealers in treasury issues subject to daily monitoring by the Federal Reserve.

To discourage unauthorized and unrecorded transactions (personal trading with association assets), the authorizing officer should initiate book entries for transactions by memo to the paying officer who books the transaction. Both parties perform their part of the transactions simultaneously on the clearing day. Therefore, all securities transactions should be delivery versus payment.

Most associations hold securities in safekeeping under delivery versus payment procedures. Management should permit free deliveries; those not requiring payment (such as a transfer from one safekeeping agent to another), only under contract specified dual approval to deter theft of the portfolio. When the association holds negotiable securities on premises, the securities should be under strict dual control at all times. Refer to [Handbook Section 540, Investment Securities](#).

### *General Lending*

To control the income from loan originations, management should provide a written schedule of fees and interest rates for originators to follow. Loan administration personnel should test loan originations to assure compliance with policy. Associations must establish a lending limit in accordance with 12 CFR § 560.93, Lending limits, to prevent overlending to any one borrower. Loan administration should enforce the limit by ensuring that it does not fund loans in excess of the association's legal lending limit. The internal auditor should report any excess loans to the board of directors.

Management should base the allowance for loan and lease losses (ALLL) on an internal asset review (IAR). They should then periodically review the credit quality and collectability of the association's loans and leases. Staff members that review and grade assets as part of the IAR should not be responsible for originating or servicing activities.

Loan originators may request loan disbursements. Until loan administration verifies that the disbursement is in agreement with the contract and the loan complies with policies, management must not authorize the disbursement. Loan administration staff should obtain and verify credit information. They should not be involved in the loan origination. These are essential segregation of duties preventing loan officers from misapplying funds.

Internal lending limits are an extremely important control. The board of directors should implement all of the following safeguards:

- Set low individual lending limits for all officers.
- Require two or more officers to co-approve larger loans.
- Require advisory committees to co-approve especially complex or very large loans.

All loans not meeting strict board approved limits and policies should require prior board approval before commitment or funding.

A central loan (or liability) ledger should tie together all direct and indirect credits and commitments for each borrower. Otherwise, the association runs a risk of lending too much to one borrower in violation of internal policies or regulations.

### *Construction Lending*

Construction lending involves many disbursements to cover construction costs as construction progresses. The association must have a construction inspector on site to verify that requests for funds (draws) are legitimate. The inspector should check to make sure material is on site and that the contractor follows construction plans. It is also prudent to occasionally alternate inspectors at each site. Their supervisor should occasionally perform a review inspection to ascertain that inspections are reliable. Before disbursement of funds, loan administration should match inspection reports to draws. They should compare them with construction plans to ensure that work is progressing accordingly. Loan administration should never authorize cash disbursements.

Staff should not make payments to third parties directly. To prove that a borrower received funds, the appropriate staff should make the payments to the borrower's account for payment of specific draws. Checks, however, may be payable jointly to the borrower and a supplier or subcontractor. When a contractor provides paid bills and materialmen's lien waivers, staff should compare them with draws to be certain that the loan funds will pay for actual expenses. Loan administration should compare progress from draws with construction plans to ensure that they are not funding cost overruns without due consideration. Refer to [Examination Handbook Section 213, Construction Lending](#).

### *Loan Servicing and Recordkeeping Functions*

After loan approval, staff should take the following steps:

- Maintain records under careful control to ensure that collection will be possible if legal action is necessary.
- Keep all collateral secure, so it cannot be lost, stolen, or released to the borrower early.
- Place large dollar collateral under dual control so that employees do not release it in error or through collusion with a borrower.
- Maintain complete collateral documents to ensure perfected collectible liens.
- Control advance payments on loans with appropriate accounting procedures.
- Whenever possible, cross-collateralize loans with the same obligor, that is, all collateral should cover all loans of the obligor.

Loan administration must be careful to adjust interest rates according to contracts. Collection efforts should follow official procedures to avoid legal complications. Collectors should keep a log of all contacts with delinquent borrowers, detailing any promised action. Management should use insurance ticklers to ensure that borrowers pay insurance premiums on time.

### *Accrued Interest Receivable*

To prevent diversion of interest earned by the association and to ensure that interest calculations are correct, the appropriate staff should perform audit tests on interest calculations.

### *Advance Payments by Borrowers for Taxes and Insurance*

Borrowers often make regular payments to an association for real estate taxes and insurance on collateral real estate. The association credits these funds to escrow or impound accounts. Staff should analyze these accounts annually to make sure the association is receiving adequate funds to cover the next expense payments. As a further control practice, the association should send the borrower an annual statement of escrow account activity. It should involve the audit department in any customer disputes. Refer to the Mortgage Banking sections of this Handbook.

### *Loans in Process*

The association typically places funds allocated for construction loans in a “loans-in-process” (LIP) account and pays draws from this account. Management should review, approve, and audit draws from LIP to ensure proper application of funds. [Refer to Examination Handbook Section 213, Construction Lending.](#)

### *Commercial Lending*

The variety and risks of commercial lending require administrative controls on both information and collateral. Management should put a tickler system into operation to ensure timely requests for financial statements from borrowers and guarantors, and to track exceptions. Qualified persons should evaluate collateral and appraise it for adequacy. Management should control collateral release to prevent loss from untimely release. Refer to [Examination Handbook Section 214, Other Commercial Lending.](#)

### *Other Loans (unsecured, mobile homes, etc.)*

Loan administration must control the entire process of lending and collecting. When a government agency is involved in a loan, the association must strictly meet the requirements for the guarantee or participation or the agency is generally relieved of duty to honor the guarantee. The association should verify the amount of Federal Housing Administration reserve accounts annually with the Department of Housing and Urban Development.

Dealer paper refers to loans originated by a retail seller of merchandise that the association funds or purchases. In funding such loans, management must maintain strict segregation of duties to avoid loss, because the association has no control over the dealer’s employees. The association must record collateral liens according to state law before another creditor records a lien. Management should inform the board of directors of charge-offs and recoveries to ensure that diversion of funds does not occur. The association must control and inspect collateral, because unlike real estate, merchandise is moveable. A financially healthy dealer can deteriorate quickly in an adverse economy. Thus, management should control collateral and carefully inspect it, since it may become the only source of payment.

Many manufacturers of mobile homes and other consumer items may have a variety of dealer financing plans that can distort the true dealer cost through rebates and volume discounts. Lending based on an invoice is, therefore, very risky. If the association finances inventory, the association must be familiar with the current wholesale market value of such inventory. Refer to [Examination Handbook Section 216, Floor Plan and Indirect Lending.](#)

### *Credit Quality Review*

Credit quality review, also known as the internal asset review or the internal classification review, is a vital credit quality control program. Refer to [Examination Handbook Section 260, Classification of Assets.](#)

### *Deposit Account Loans*

Losses can be serious if the association does not adequately control loans secured by deposit accounts. Lack of control may result in serious problems. These problems include:



- Forged signatures on the loan documents.
- Misapplication of loan proceeds.
- Withdrawal of collateral deposits without paying the loan. Refer to [Examination Handbook Section 560, Deposits/ Borrowed Funds](#).

#### *Real Estate Owned and Other Repossessed Assets*

The association must establish ownership of real estate, acquired because of debts previously contracted, according to local laws and customs under legal advice. Accounting practices require a prompt appraisal to determine the correct carrying value of the new association asset. Management must periodically inspect properties for needed maintenance to limit deterioration. If properties have material value, the association's management should bond collection and management agents, or at least ensure that they are bondable. The association should acquire hazard insurance, when available. Refer to [Examination Handbook Section 251, Real Estate Owned and Other Repossessed Assets](#).

#### *Real Estate Held for Investment*

Management should control each parcel separately to provide for informed decisions to hold or sell. They must maintain accounting controls to create reliable records. Refer to [Examination Handbook Section 230, Equity Investments](#), for more comments.

#### *Fixed and Other Assets*

While these assets may not require as much attention as others, management must maintain routine accounting controls as support for the general ledger and tax returns. Refer to [Examination Handbook Section 250, Other Assets/Liabilities](#), and [Section 252, Fixed Assets](#).

#### *Deposit Accounts*

Due to the high volume of activity in deposit accounts, management may streamline routines for convenience and to minimize expense. To limit loss from errors and irregularities, management must ensure that controls are in place to recognize unusual transactions and limit loss. These controls should include:

- Officer approval and reviews for propriety regarding any unusually large transactions.
- Routine procedures and activity reviews that ensure segregation of duties and confirm transactions with customers when they open and close deposit accounts.
- Reconciliation of deposit ledgers to the general ledger daily.
- Testing of interest calculations periodically to ensure correctness.
- Testing of accrued interest accounts for adequacy to ensure no misapplication of funds, or under accrual of expense.

- Dual control of all deposit accounts used as collateral to prevent inappropriate withdrawals.
- Periodic advertisement of unclaimed balances.
- Crediting unclaimed balance accounts to the State according to State escheat laws. (Escheat laws limit the build-up of dormant accounts). Refer to [Examination Handbook Section 560, Deposits/ Borrowed Funds](#).

Review of check kiting reports.

Service providers normally provide a check-kiting report (for example, “Kiting Suspect Report”) to associations that identifies potential check-kiting situations. The report shows those accounts with activity indicating the drawing upon uncollected funds, and the recurring presence on the report by an account holder could indicate a kiting situation. However, the parameters for these reports may vary depending on whether the service provider allows the association to set up specific parameters; otherwise, a default setting may be used. Most of the account holders identified on the report are not involved in check kiting, but it does provide management with a good overview of the operation and possible check kiting. The service provider usually runs the report on a daily basis. Someone who does not have access to teller operations should review the report.

#### *Deferred Credits*

Generally accepted accounting principles require recognition of loan origination fees as income over the life of the loan in accordance with SFAS No. 91. The association should carry such deferred income as a deferred credit. See the [Examination Handbook Section 251, Real Estate Owned and Other Repossessed Assets](#), for comments on accounting conventions for sale of these assets.

#### *Other Liabilities*

Management should periodically review miscellaneous accounts to deter misuse. These accounts should be minimal.

#### *Capital (Reserves, Undivided Profits, etc.)*

Management must carefully control all changes in the ownership records of the association through the officially designated registrar. Management should report all capital account entries to the board of directors. Refer to [Examination Handbook Section 110, Capital Stock and Ownership](#).

#### *Letters of Credit*

These credit documents require strict controls similar to loans. Although letters of credit do not appear on balance sheets, they can result in liabilities for payment. A bona fide commitment for a letter of credit generally carries the same contingency for liability as a letter of credit, if the holder can prove the authenticity of the commitment. Refer to the [Examination Handbook Section 215, Letters of Credit](#), for additional discussion.

## Funds Transfer Questionnaire

The transfer of funds is an essential activity for all depository institutions. It is, however, a source of extreme vulnerability to material loss from mistakes and fraud if not adequately controlled. Control procedures and fidelity bond coverage can limit the risk to capital. However, management should not use the bond deductible and coverage as a substitute for adequate controls. A quick review of the blanket bond deductible and coverage amount and any related policy riders will give you an idea of the reliance the association places on control procedures to limit risk from funds transfer activities.

In your review, you should ascertain the following information:

- Whether the transfers pose risk to capital.
- Whether management prescribes reasonable controls.
- That management confirms or tests the controls periodically.

Use of the Funds Transfer Questionnaire and examination procedures should provide you with enough information to make a reliable judgment on the adequacy of transfer controls.

This Appendix discusses the following:

- Background information.
- The transfer process.
- Common effective control procedures.

### Background Information

Transfers may originate internally or externally. They can be among internal accounts or external accounts and can involve one customer or many customers. Essentially, all transfers are instructions by an authorizer to debit an account at an institution for credit to another account at either the same or another institution.

For this discussion, funds transfer includes the transfer of control over funds, both internal and external, to an association. Two common examples of internal transfers are: loan fundings and deposit transfers among customers' accounts in the association. External transfers are payments involving more than one depository institution.

All associations engage in transfers. Most are involved in large transfers relative to their capital accounts, and blanket bond coverage with deductibles. Associations without correspondent banking departments and major corporate deposit accounts may not have a large volume of transactions.

Many routine control procedures exist that can limit risk from funds transfer activities. The procedures in use must be compatible with the following parameters:

- The volume of activity the association expects related to capital.
- Insurance coverage and deductibles.
- The size and diversity of the association's staff.

Association management must ensure that staff encrypts all data transmissions using algorithms. This protects information from improper disclosure or alteration. You can find additional text on electronic funds transfer systems in the Federal Financial Institutions Examination Counsel (FFIEC) Information Technology Examination Handbook. However, it does not address control procedures required by funds transfer activities.

#### Transfer Process

Associations execute internal transfers through the accounting system. Internal transfers may be initiated on paper, by direct key entry, or through other computer links.

Associations may execute external transfers through any of the following means:

- Official (drawn on us) checks
- Drafts on correspondent accounts
- Customer depository transfer checks
- Customer checks or drafts
- Computer link to independent transfer systems
- Direct computer link to a correspondent
- Voice telephone (voice transmission) call to a correspondent.

Transfers may use various transmission mediums such as:

- Dial-up common carrier lines (telephone, telex, electronic mail)
- Dedicated lines
- Hard-wire terminals requiring no dial up
- Paper text
- Electronically transmitted-image facsimile (FAX)
- Voice

- Encrypted data.

These mediums may use various technologies such as wires, radio phone, cellular radio telephone, microwave, or fiber optic lines, each with different security and vulnerability. There are several wire transfer service providers:

- Fedwire
- CHIPS
- SWIFT
- The Federal Home Loan Banks
- Other correspondent banks
- Electronic mail services.

Each medium, method, technology, and service has strengths and weaknesses, and none are perfect.

#### Common Effective Control Procedures

A customer or association employee may initiate a transfer, which debits the customer's account. Appropriate association personnel must verify that the account holder authorized the customer debit. Management must ensure that authorizations include a written contract specifying how, when, and who can initiate transfers. A depository contract on a signature card may also detail authorizations. Authorizations may be specific or general. General authorizations may be blanket for any amount or repetitive for the same amount. A general authorization must include who may make transfers, how much the transfers can be, and when the transfer can occur.

Appropriate staff should record general authorizations in system controls for automatic confirmation of authorization. General authorization controls may require initiator and sender identification codes, unique passwords, cipher codes, set procedures, and limited channels of communication. Appropriate staff must initiate requests for transfers using contractually agreed upon means permitting confirmation before execution.

Preferably, before a sender executes any transfer requests originating in the association, appropriate association personnel must verify the initiator's authorization and provide an approval to the sender. Management should segregate the duties of initiating and executing a transfer. If prior approval is not practical, then management should establish a transaction ceiling – an amount above which a lack of prior approval will stop the transfer.

After execution of the transfer, appropriate association personnel should send notice of transfers to the account holders' address of record. Someone other than the initiator or executor should send the confirmation to prevent tampering. The initiator or another person should review transfer accounting entries for authenticity by comparing the transfer accounting entry with the approved request.

It is very important that funds transfer approval levels increase proportionately with the amount of the transfer. For example, for transfers less than \$10,000, staff members or junior officers may make approval. For amounts of \$50,000 to \$100,000, a junior officer may authorize the transfer once they determine the transfer is valid. For amounts greater than \$100,000, the association should require dual officer approval. For amounts greater than \$1 million, dual senior level officers should approve the transfer with required callbacks from the receiving bank.

An example of a typical transfer is a customer phoning a request to transfer funds from a savings account to a checking account. The customer is an authorized drawee on both accounts. This is not problematic provided control procedures ensure that the authorizing customer is a drawee on both accounts. Management should instruct association employees to verify that a drawee authorized, in writing, any requested transfer from one customer's account to another customer's account, prior to making the transfer. Large or unusual transfers should require higher level or approval before execution. Subsequent controls should include either a review of debits to ascertain that the debit and credit are between accounts with a common drawee, or that both an initiator and an approver have confirmed the drawee's authorization of the transfer.

To avoid misunderstandings with multiple drawee accounts, a drawee should sign a written authorization indicating that the association should honor telephone requests for transfers between accounts. Management should ensure that employees maintain a file of the written authorizations.

A typical two-party transfer is a debit to a checking account and credit to a utility or other creditor for a monthly billing. The appropriate employee executes the transfer using a draft supported by an authorization. Another typical two-party transfer is a debit to a loan or loans process account and a credit to a supplier or contractor. For all transfers from one drawee's account to another drawee's account, the association should have a written authorization or request from a drawee. The written authorization or request should specify the following information:

- The amount the drawee wants transferred.
- The account to debit (charge, or transfer money from).
- The account to credit (transfer money to).

The authorization may cover several specific transfers, a series of transfers, or one transfer.

Follow-up controls should include confirmation of signatures on authorizations or requests. A person independent of the initiation of a request should be involved in either the approval or the confirmation process. This assures segregation of duties and limits opportunities for collusion. For example, the initiator and sender of transfers should be separate; one individual should initiate the securities transaction while another individual executes it. Payment (settlement) should only occur upon confirmation of the initiated order to the executed trade ticket.

Transfers of funds outside of the association (external transfers) must be through accounts of the association at correspondents. The appropriate association personnel should initiate the transfer through regular communication channels.

Daylight overdrafts are overdrafts existing between the daily closing of accounting records. Even when daylight overdrafts are properly controlled, they are a credit risk. If inadequately controlled, daylight overdrafts may be a very serious transfer risk. When a correspondent permits daylight overdrafts, funds available for transfer may be virtually unlimited and may be unrecoverable. To facilitate maximum volume of transactions, controls on daylight overdrafts usually do not prevent excessive over drafting; instead, they stop continued over drafting after the association exceeds a certain limit. For this reason, internal controls on external transfers must be rigid and subject to frequent testing and review to discourage and prevent loss.

Refer to [Examination Handbook Section 580, Payments System Risk](#), for discussion of the setting of limits for daylight overdrafts.

A low-volume voice transmission operation must also have rigid controls. Voice recognition alone is unacceptable as a control. Generally, there is no witness to verify recognition and no call back to verify the location of the caller. Typical controls require a four party callback or confirmation process on all external transfers. For example, once the association receives a customer request, appropriate personnel must confirm the request as authorized in writing by the customer, and approve it as confirmed. The sender then executes the request by transmission to a correspondent. The usual means is by a telephone call. The correspondent receiver hangs up the phone, and has an approver confirm the transfer request with a separate confirmer at the association, usually by a telephone call back. This process must involve four persons (two at each institution) to be a valid control procedure. It relies on segregation of duties to prevent collusion at either institution. Management should implement the following additional steps:

- Provide each person with a recognizable identity such as a name, code word, or number.
- Identify each transfer by sequence number known to both the sender and receiver.
- Record all calls.

Segregation of duties requires that wire transfer senders not be initiators or approvers. Senders should always look for the required approvals before sending a message. To control wire transfers, someone not involved in either initiating, approving, or sending messages should frequently review all messages. In low-volume PC operations, daily review of an unbroken printout of all messages (comparing the record of messages with the approved request forms) is a common control review.

Other common control safeguards include the following procedures:

- Limited signing authorities.
- Dual controls over forms.
- Supervisor's key controls on computer terminals.
- Unique passwords for transfer clerk (sender) and releaser.

It is common for institutions to number each message with an encoded sequence number and require use of a confidential test key to decode the number. For this control procedure to have integrity, the holders of the test key should not have the ability to send or receive messages.

Management may require additional controls, such as limiting the funds available for transfer. Correspondent banks require this procedure for extremely weak institutions to prevent daylight overdrafts on respondent accounts. A correspondent relationship may also require that the institution make all outgoing transfers from one specific account not used for incoming transfers. In addition, the correspondent banks may not permit daylight overdrafts. This procedure requires the sending association (respondent) to transfer funds from an operating account at the correspondent to a transfer account before transferring funds to another institution. The first transfer request makes funds available for transfer. The second transfer request executes the external transfer.

Someone without signature authority should control supplies of negotiable forms such as single signature official checks and drafts. This person must require an authorized voucher for release of a check or draft, preferably after it is prepared for signature. The appropriate staff should reconcile paid official checks to accounting records of vouchers and review them for authorized signatures.

Whenever check-signing procedures use signature machines, the signature plates should be under key control at all times, with dual control on dual signature machines and plates. Daily control procedures should include reconciling the signature counter totals to the number of check authorizations to ascertain that no one signed extra checks.

Daily independent reconciliation of wire transfers with correspondent accounts and general ledger accounts is an essential control to ensure detection of any errors or misapplications of funds. Any chances of retrieval of missent funds diminish quickly. You should check whether the institution has routines that require action by two people to complete a transfer, one to receive or initiate the request and another to confirm authenticity. If the association makes transfers to offshore privacy havens, determine how management investigates the transfer for legitimacy.

Due to the detail involved, you should review the internal controls on funds transfers by interview and observation rather than by audit methods. Any procedures allowing one person to remove unlimited funds from an account without immediate detection should receive report comment and follow-up at the next examination. Initiate enforcement action to correct unsafe and unsound operating procedures whenever association management is uncooperative in resolving inadequate controls.



**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As of Date: >**

A management official of the association should complete this questionnaire. If the association lacks an effective system of internal audit or control, the examiner should verify appropriate responses and initial in the verified column. The flagged questions are the suggested minimum verifications. Management must provide the examiner with an adequate written explanation of all “No” answers, with an appropriate reference to the question, and supply copies of applicable written procedures. If a question is not applicable to the association, respond with NA.

**Internal Audit** [11]

	Verified by Examiner		Yes	No
_____	1.	Does the association have an internal audit program?	_____	_____
_____	2.	Do the internal audit programs contain written, specific instructions for audit procedures for the internal auditor to perform?	_____	_____
_____	3.	Does the board of directors or the audit committee review internal audit reports?	_____	_____
_____	4.	Does the audit committee consist only of outside directors?	_____	_____
_____	5.	Do internal audit reports suggest actions to correct internal control or procedural deficiencies?	_____	_____
_____	6.	Is there a subsequent review to ascertain that the association implemented suggestions for corrective actions?	_____	_____
_____	7.	Does the internal auditor report to or receive salary reviews by the audit committee or board of directors?	_____	_____
_____	8.	Did the external auditor communicate any reportable conditions, either orally or in writing, to management, the board of directors, or the audit committee?	_____	_____

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

**General Items** [12]

- \_\_\_\_\_ 9. Does the association reconcile the following accounts to the general ledger at least daily (if activity is minimal, weekly or monthly reconciliations may be appropriate)? \_\_\_\_\_
- Loans in process
  - Suspense accounts
  - Accounts out of balance
- \_\_\_\_\_ 10. Does the association reconcile the following accounts to the general ledger at least monthly? \_\_\_\_\_
- Loans
  - Investment securities
  - Real estate owned
  - Borrowings
  - Checking and deposit accounts
- \_\_\_\_\_ 11. Does a person not involved in general ledger entries perform the reconciliations? \_\_\_\_\_
- Person responsible? \_\_\_\_\_
- \_\_\_\_\_ 12. Does a person not involved in the transactions periodically review and investigate activity on exception and/or large items report(s)? \_\_\_\_\_
- Person responsible? \_\_\_\_\_
- \_\_\_\_\_ 13. Does the association perform a regular review of insider activity for unusual activity and compliance with Regulation O? \_\_\_\_\_

**INTERNAL CONTROL QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 14. Does the association appropriately capitalize and expense all items?   | _____ | _____ |
| _____ | 15. Does the association periodically review deferred asset and liability accounts?  | _____ | _____ |
| _____ | 16. Does the association clearly show the nature and purpose of each entry to the deferred asset and liability accounts?                         | _____ | _____ |
| _____ | 17. What is the name and position of the person authorized to make entries to the deferred asset and liability accounts?                         |       |       |
|       | Person responsible? _____  |       |       |
|       | Position of person? _____  |       |       |
| _____ | 18. Does the association balance and reconcile to third-party reports monthly any association assets that others service or hold in safekeeping? | _____ | _____ |
|       | Person responsible? _____  |       |       |












**Cash and Cash Items<sup>[13]</sup>**

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 19. Does the association reject checks when the collected balance of the customer's demand deposit account is not sufficient to cover the item? | _____ | _____ |
| _____ | 20. Are all personnel who have cash approval and disbursement authority required to take annual vacations of at least two consecutive weeks?    | _____ | _____ |
| _____ | 21. Does an independent officer review all overdraft activity?  | _____ | _____ |
|       | Person responsible? _____   |       |       |
| _____ | 22. Are controls in effect to prevent withdrawals of uncollected funds?   | _____ | _____ |
| _____ | 23. Does the association promptly record on the books returned items previously deposited?  | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**


Verified By Examiner		Yes	No
-------------------------	--	-----	----


- |   |   |                    |                    |
|---|---|--------------------|--------------------|
| <br>_____<br>_____   | 24. Are procedures adequate to ensure that the association monitors and clears uncollected items?<br><br> Person responsible? _____  | _____<br><br>_____ | _____<br><br>_____ |
| _____<br>_____  | 25. If the association maintains a petty cash fund, are all additions and withdrawals documented?<br><br>26. Does the association balance the petty cash fund periodically?   | _____<br><br>_____ | _____<br><br>_____ |
| _____<br>_____  | 27. Does the association have procedures that prevent the use of liquid assets as compensating balances or collateral for personal loans of officers, directors, or employees?<br><br>28. Does the association record cash items appropriately in the general ledger?   | _____<br><br>_____ | _____<br><br>_____ |
| <br>_____<br>_____ | 29. Does the association review teller and accounting system override reports and file maintenance summaries for unusual activity on a regular basis?<br><br> Person responsible for accounting overrides? _____<br><br> Person responsible for teller overrides? _____ | _____<br><br>_____ | _____<br><br>_____ |
| <br>_____          | 30. Are loan accounting systems included in the override reports?   | _____              | _____              |
| <br>_____          | 31. Are personnel who have control over cash barred from performing overrides?  | _____              | _____              |
| <br>_____          | 32. Do only designated personnel who have no control over cash approve and review overrides?  | _____              | _____              |
| <br>_____          | 33. Does the association, at both home and branch offices, perform daily cash reconciliations?  | _____              | _____              |
| <br>_____          | 34. Does a person without teller responsibilities perform the daily cash counts?  | _____              | _____              |
| <br>_____          | 35. Are overages and shortages properly recorded in a cash over and short account?  | _____              | _____              |


**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As Of Date:**>


Verified By Examiner		Yes	No
-------------------------	--	-----	----


 \_\_\_\_\_ 36. Does the association maintain records showing the person involved in the cash over or short situation? \_\_\_\_\_

 \_\_\_\_\_ 37. Does the association investigate and act upon all cash over and under amounts? \_\_\_\_\_


 \_\_\_\_\_ 38. Does the association have appropriate controls over unissued deposit certificates, travelers' checks, savings bonds, food stamps, and other consigned items? \_\_\_\_\_


 Person(s) responsible? \_\_\_\_\_


 \_\_\_\_\_ 39. Does the association periodically reconcile consigned items? \_\_\_\_\_


 Person responsible? \_\_\_\_\_


**Association (Official) Checks** <sup>[14]</sup>


 \_\_\_\_\_ 40. For checks signed by hand: Are two signatures (signer and approver) required on association (official) checks? \_\_\_\_\_


 Names of persons authorized to sign? \_\_\_\_\_

 \_\_\_\_\_ 41. For checks signed by hand: Are unsigned blank checks in the possession of an officer or employee who does not have singular signature authority? \_\_\_\_\_

 Responsible officer or employee? \_\_\_\_\_

 Position title? \_\_\_\_\_

 \_\_\_\_\_ 42. For checks signed by stand-alone mechanical or electronic facsimile check signing machines connected to computers: Is the inventory of unsigned blank checks available verified daily and compared to the work of other positions that issue checks during the day? \_\_\_\_\_

 Person(s) responsible? \_\_\_\_\_

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |               |   |              |              |
|---------------|---|--------------|--------------|
| <p> _____</p> | <p>43. For checks signed by stand-alone mechanical or electronic facsimile check signing machines connected to computers: Is there an approval process for checks in excess of a certain dollar amount?</p> <p style="margin-left: 40px;">➡ If so, what is the amount? _____</p>  | <p>_____</p> | <p>_____</p> |
| <p>_____</p>  | <p>44. For checks signed by stand-alone mechanical or electronic facsimile check signing machines connected to a computer: Is the association's copy of the check voucher initialed by the person preparing the check and, for those checks in excess of a certain amount, initialed by a person authorized to approve?</p> | <p>_____</p> | <p>_____</p> |
| <p>_____</p>  | <p>45. Does the association have controls in place to ensure that the employee fills out the amount of the check and payee information before the signatures are on the checks?</p> <p style="margin-left: 40px;">➡ Person responsible? _____</p>   | <p>_____</p> | <p>_____</p> |
| <p>_____</p>  | <p>46. Is the supply of unused checks periodically reconciled to the shipping invoice by persons without signature authority?</p> <p style="margin-left: 40px;">➡ Person responsible? _____</p> <p style="margin-left: 40px;">➡ How often? _____</p>  | <p>_____</p> | <p>_____</p> |
| <p> _____</p> | <p>47. Does a person independent of the check writing function review the paid (canceled) checks for proper signatures and reconcile the check to vouchers?</p> <p style="margin-left: 40px;">➡ Person responsible? _____</p> <p style="margin-left: 40px;">➡ How often? _____</p>  | <p>_____</p> | <p>_____</p> |
| <p> _____</p> | <p>48. Does the association periodically reconcile outstanding checks to vouchers and liability accounts?</p>   | <p>_____</p> | <p>_____</p> |
| <p>_____</p>  | <p>49. Does the association periodically transfer all outstanding six-month old association checks to a liability account?</p>  | <p>_____</p> | <p>_____</p> |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

\_\_\_\_\_ 50. Does the association keep the facsimile check writing machine under proper control? \_\_\_\_\_

***Due From Banks.*** [15]

\_\_\_\_\_ 51. The association receives bank statements:  
 Daily \_\_\_\_\_ Monthly \_\_\_\_\_ Quarterly \_\_\_\_\_

\_\_\_\_\_ 52. Does the association reconcile bank accounts on a regular and timely basis? \_\_\_\_\_

\_\_\_\_\_ 53. Are there any unreconciled bank accounts? \_\_\_\_\_  
 If so, what is the date of the latest reconciliation? \_\_\_\_\_

\_\_\_\_\_ 54. Are there are any out of balance accounts? \_\_\_\_\_  
 If so, what is the date the association expects it to be reconciled?  
 \_\_\_\_\_

\_\_\_\_\_ 55. Is the person who reconciles the bank statements independent of the deposit and check writing process? \_\_\_\_\_  
 Person responsible? \_\_\_\_\_

\_\_\_\_\_ 56. Do checks drawn on bank accounts need more than one signature? \_\_\_\_\_

\_\_\_\_\_ 57. Does a person who does not have signature authority periodically reconcile unsigned checks to the shipping invoice? \_\_\_\_\_  
 Person responsible? \_\_\_\_\_  
 How often? \_\_\_\_\_






**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**


**Docket #: >**


**Institution Name: >**

**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

 \_\_\_\_\_ 67. Does a person who does not execute or book transactions receive confirmations from the broker/dealer? \_\_\_\_\_

 Person responsible? \_\_\_\_\_


 \_\_\_\_\_ 68. Does a person without transaction authority receive monthly statements direct from the brokerage firm indicating all transactions during the period? \_\_\_\_\_

 Person responsible? \_\_\_\_\_


\_\_\_\_\_ 69. Are all securities transactions for delivery versus payment? \_\_\_\_\_

\_\_\_\_\_ 70. Does the association prohibit “free” deliveries in written contracts with depositories and safekeeping agents unless approved by two senior officers? \_\_\_\_\_


\_\_\_\_\_ 71. Does the association hold securities on the premises under dual control? \_\_\_\_\_

 \_\_\_\_\_ 72. Is an independent party performing tests to determine that the yield on investments actually received is in line with the weighted average coupon of such assets? \_\_\_\_\_

 Name of the independent party: \_\_\_\_\_

 How often: \_\_\_\_\_

 Date of last test: \_\_\_\_\_

 Period analyzed: \_\_\_\_\_

**General Lending** <sup>[17]</sup>

\_\_\_\_\_ 73. Does the association have and adhere to a written schedule of fees and rates charged on new loans? \_\_\_\_\_

\_\_\_\_\_ 74. Does the association policy limit the number or amount of loans involving any individual borrower or contractor? \_\_\_\_\_

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 75. Is there a procedure of internal review to ensure compliance with the above policy by a person or persons who are independent of the loan approval function?   | _____ | _____ |
| _____ | 76. Are there procedures, and does staff follow the procedures, to periodically review and document the adequacy of the ALLL?  | _____ | _____ |
| _____ | 77. Are the persons that periodically review and document the adequacy of the ALLL independent of the loan approval function?  | _____ | _____ |
| _____ | 78. Does the association defer loan fees in accordance with generally accepted accounting principals (GAAP), and not recognize fees as current-period income?  | _____ | _____ |
| _____ | 79. Are lending officers prohibited from authorizing loan disbursements?   | _____ | _____ |
| _____ | 80. Do persons independent of the loan officer obtain or verify credit information?  | _____ | _____ |
| _____ | 81. Are lending authorities, granted by the board of directors, setting tiered dollar limits for individuals, co-approval limits for committees, and higher limits for approval by the board of directors? | _____ | _____ |
| _____ | 82. Is there a record system that lists the total of outstanding credits and commitments (direct and indirect) for each borrower?  | _____ | _____ |

**Construction Lending<sup>[18]</sup>**

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 83. Are inspectors rotated at least every third inspection and for final draws?                                | _____ | _____ |
| _____ | 84. If the association does not rotate inspectors, does the inspector's supervisor perform review inspections? | _____ | _____ |
| _____ | 85. Is there segregation of duties between inspection and disbursement functions?                              | _____ | _____ |
| _____ | 86. Does the association prohibit disbursing loans in cash or to third parties?                                | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 87. Does the association compare paid bills and lien waivers with items listed for disbursements?                          | _____ | _____ |
| _____ | 88. Does the association have safeguards to ensure that sufficient funds always remain available to complete construction? | _____ | _____ |

***Loan Servicing and Recordkeeping Functions*** <sup>[19]</sup>

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 89. Does the association support advances by written evidence or re-inspection of property?   | _____ | _____ |
| _____ | 90. Are all notes and other loan documents kept in a vault or fire-resistant cabinet and under a sign-out control system?                                   | _____ | _____ |
| _____ | 91. If the association holds additional collateral, do they safeguard it?   | _____ | _____ |
| _____ | 92. Does the association maintain a record of such collateral?  | _____ | _____ |
| _____ | 93. Does the association obtain written acknowledgment from the borrower for the pledging of savings accounts or the assignment of life insurance policies? | _____ | _____ |
| _____ | 94. Does the association adequately control advance loan payments if they do not immediately credit the advance to the loan account?                        | _____ | _____ |
| _____ | 95. Does the association test periodic adjustments to adjustable-rate mortgage loans for compliance with the terms of the note?                             | _____ | _____ |
| _____ | 96. Does the association have written collection policies and procedures that the board of directors approves?  | _____ | _____ |
| _____ | 97. Do collectors document the contact with borrowers and indicate promised action?   | _____ | _____ |
| _____ | 98. Are there procedures that ensure the maintenance of necessary hazard, flood, and other insurance coverages throughout the life of the loan?             | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**


**Docket #:** >

**Institution Name:** >

**Examination As Of Date:**>

Verified By Examiner		Yes	No

**Accrued Interest Receivable** [I10]

- \_\_\_\_\_ 99. Does the association perform tests to determine that it is receiving the appropriate interest? \_\_\_\_\_
- \_\_\_\_\_ 100. Does a person, independent of the cash receipt and bookkeeping for interest receivable, perform and document an analysis to determine if the yield on mortgages and investments actually received is in line with the weighted-average coupon rate of such assets? \_\_\_\_\_
-  \_\_\_\_\_ 101. Are accounting entries for accrued interest receivable supported by proper explanations evidencing the nature and purpose of each entry and signed by a responsible individual? \_\_\_\_\_

**Advance Payments by Borrowers for Taxes and Insurance** [I11]

- \_\_\_\_\_ 102. Is each escrow (impound) account analyzed at least once a year to ensure that the payments will cover the disbursement(s)? \_\_\_\_\_
- \_\_\_\_\_ 103. If this analysis results in a revision of monthly payments, is the revision made promptly and the borrower notified? \_\_\_\_\_
- \_\_\_\_\_ 104. Does the association inform borrowers at least annually of the balance in their account and the most recent year's transactions in that account? \_\_\_\_\_
- \_\_\_\_\_ 105. Do statements indicate that borrower's disputes regarding the balances of their escrow accounts be sent to internal audit or a department independent of escrow transactions? \_\_\_\_\_

**Loans in Process** [I12]

- \_\_\_\_\_ 106. Are loans in process reviewed periodically to determine whether the association makes disbursements on a timely basis and in accordance with the terms of loan agreements? \_\_\_\_\_
- \_\_\_\_\_ 107. Do personnel not responsible for the loans in process accounts conduct periodic tests to determine propriety of disbursements? \_\_\_\_\_

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As Of Date:**>

Verified By Examiner		Yes	No
-------------------------	--	-----	----

**Commercial Lending** [I13]

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 108. Does the association update borrower's and guarantor's financial statements at least annually?  | _____ | _____ |
| _____ | 109. Do qualified individuals evaluate the collateral?   | _____ | _____ |
| _____ | 110. Does the association inspect collateral periodically to ensure maintenance of sufficient value?   | _____ | _____ |
| _____ | 111. Does the association release collateral only upon the approval of an officer or committee having a lending limit greater than or equal to the value of the collateral the association is releasing? | _____ | _____ |
| _____ | 112. If the association releases collateral upon payment of the loan, do they release the collateral only upon receipt of collected funds?   | _____ | _____ |

**Other Loans (unsecured, mobile homes, etc.)** [I14]

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 113. Are the association's procedures adequate to ensure compliance with the requirements of any government agency insuring or guaranteeing the loan?  | _____ | _____ |
| _____ | 114. Does the association maintain an adequate loan register?<br><br>The register, as a minimum, should contain the following: loan number, loan amount, date of loan or date of purchase, dealer, recourse or repurchase provisions, interest rate, and term. | _____ | _____ |
| _____ | 115. Do personnel who do not handle cash process loan applications and initial the notes?  | _____ | _____ |
| _____ | 116. Do employees not connected with the granting or acquisition of loans collect and process receipts, and prepare delinquency lists?   | _____ | _____ |
| _____ | 117. Are liens and other documents, including titles, promptly recorded?   | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**






Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 118. Are there procedures that provide for board of directors approval of charge-offs and subsequent recoveries?  | _____ | _____ |
| _____ | 119. If the association holds additional or side collateral for unsecured loans, does the association also adequately document and safeguard the collateral and maintain a proper record?                             | _____ | _____ |
| _____ | 120. Does the association reference the FHA publication that lists companies and individuals who have not properly performed under FHA programs?  | _____ | _____ |
| _____ | 121. Floor planning loans:  | _____ | _____ |
|       | Does the association make unannounced inventory inspections on a rotating basis at least every 30 days?   | _____ | _____ |
| _____ | Do the inventory inspections include, as a minimum, the following: serial number verification of unit, inventory of equipment and furnishings, condition and location of unit, and units sold out of trust or rented? | _____ | _____ |
| _____ | Does the association maintain records of floor plan inspections?  | _____ | _____ |
| _____ | Does the association actually inspect demos at a subsequent date, if necessary?   | _____ | _____ |
| _____ | Does the association rotate inspectors or have a supervisor or auditor accompany them?  | _____ | _____ |
| _____ | Does the association inspect and appraise trade-ins for wholesale value?  | _____ | _____ |
| _____ | Does the dealer submit financial and operating statements monthly?  | _____ | _____ |
| _____ | Does the association retain title or lien control?  | _____ | _____ |
| _____ | Do floor plan agreements provide for periodic reductions (curtailments) in outstanding unit loan balances?  | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**


Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 122. For dealer financing, does the dealer application include the following:   | _____ | _____ |
|       |  Business address and location of all sales and storage lots?  |       |       |
| _____ |  Names of all manufacturers represented and general description of units stocked?  | _____ | _____ |
| _____ |  A statement as to whether each manufacturer subscribes to the Truth in Invoicing Practices Statement adopted by the Manufactured Housing Institute? | _____ | _____ |
| _____ |  A statement as to the willingness of the dealer to sign recourse or repurchase agreements?   | _____ | _____ |
| _____ |  Name and percentage of ownership of all persons with interests in the dealership?   | _____ | _____ |

**Credit Quality Review** [I15]

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 123. Does the association have a credit quality review program?   | _____ | _____ |
| _____ | 124. Does credit quality review include testing for compliance with regulation, association policy, officer lending limits, and association underwriting standards? | _____ | _____ |
| _____ | 125. Does credit quality review include classification or grading of assets?  | _____ | _____ |
| _____ | 126. Are the findings of the persons responsible for credit quality review reported directly to the board of directors?   | _____ | _____ |

**Deposit Account Loans** [I16]

- |   |  |       |       |
|---|--|-------|-------|
| _____   | 127. Are sufficient controls in effect to prevent a loan approver from disbursing loan proceeds? | _____ | _____ |
|  _____ | 128. Does the association flag pledged deposit accounts to prevent collateral from withdrawal?   | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- \_\_\_\_\_ 129. Does withdrawal of pledged funds require a supervisory override? \_\_\_\_\_
- \_\_\_\_\_ 130. Are procedures in effect to ensure that the total loan and accrued interest does not exceed the balance amount of the deposit account? \_\_\_\_\_
- \_\_\_\_\_ 131. Are procedures in effect for initial and periodic positive mail confirmations with deposit loan customers? \_\_\_\_\_
- \_\_\_\_\_ 132. Are periodic monitoring reports adequate for the review of savings deposit loan activity? \_\_\_\_\_

**Real Estate Owned and Other Repossessed Assets** [I17]

- \_\_\_\_\_ 133. Does the association follow routine legal procedures that will result in a valid title to the property and evidence of such title? \_\_\_\_\_
- \_\_\_\_\_ 134. Does the association promptly value real estate that it acquires? \_\_\_\_\_
- \_\_\_\_\_ 135. Does the association use a current valuation to establish the sales price of a property? \_\_\_\_\_
- \_\_\_\_\_ 136. Does the association physically inspect properties at periodic intervals? \_\_\_\_\_
- \_\_\_\_\_ 137. Do such inspections indicate the condition of the property and occupancy status? \_\_\_\_\_
- \_\_\_\_\_ 138. Are there maintenance procedures in effect to ensure that properties will retain their market value? \_\_\_\_\_
- \_\_\_\_\_ 139. Does the association maintain separate subsidiary records for each parcel showing items capitalized, expenses, rentals, etc.? \_\_\_\_\_
- \_\_\_\_\_ 140. Does the association balance subsidiary ledgers for the individual properties to the general ledger at least monthly? \_\_\_\_\_
- \_\_\_\_\_ 141. Does the association maintain separate files for each parcel of real estate owned and are such files complete? \_\_\_\_\_



**INTERNAL CONTROL QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 142. Does the association maintain controls over the receipt of rental income?  | _____ | _____ |
| _____ | 143. Does the association’s advertising for the sale or rental of real estate owned comply with the provisions contained in the Department of Housing and Urban Development’s advertising guidelines? | _____ | _____ |
| _____ | 144. Are agents who collect rents and manage properties bonded?   | _____ | _____ |
| _____ | 145. Are security deposits properly controlled?   | _____ | _____ |
| _____ | 146. Does the association have procedures to ensure maintenance of hazard insurance?  | _____ | _____ |

**Real Estate Held for Investment** [118]

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 147. Does the association maintain separate subsidiary records for each parcel showing items capitalized, expenses, rentals, etc.?        | _____ | _____ |
| _____ | 148. Does the association balance subsidiary ledgers for the individual properties to the general ledger at least monthly?                | _____ | _____ |
| _____ | 149. Does the association maintain complete, separate files for each parcel of real estate owned?   | _____ | _____ |
| _____ | 150. Does the association maintain adequate control over rental income?   | _____ | _____ |
| _____ | 151. Are agents who collect rents and manage properties bonded?   | _____ | _____ |
| _____ | 152. Are security deposits properly controlled?   | _____ | _____ |
| _____ | 153. Does the association maintain adequate controls over all disbursements?  | _____ | _____ |
| _____ | 154. Does a senior officer compare disbursements to determine whether they are for budgeted purposes and in line with the overall budget? | _____ | _____ |
| _____ | 155. If not, is the board of directors notified promptly of budget overruns?  | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

**Fixed and Other Assets** [119]

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 156. Does the association retain invoices in support of all additions to fixed asset accounts?  | _____ | _____ |
| _____ | 157. Does the association ensure that the accounting department knows about any major retirement of fixed assets?   | _____ | _____ |
| _____ | 158. Does the association keep a detailed record of fixed assets?   | _____ | _____ |
| _____ | 159. Does the association retain depreciation schedules supporting each asset or class of assets?   | _____ | _____ |
| _____ | 160. Does the association charge depreciation and amortization expenses at least quarterly?   | _____ | _____ |
| _____ | 161. Does the association retain evidence of valid titles for all properties owned?   | _____ | _____ |
| _____ | 162. If the association has rented space in its buildings, does it have adequate control over the recording and collection of rental income and the control and recording of expense? | _____ | _____ |
| _____ | 163. Are there record keeping procedures to ensure that the association maintains adequate supporting documentation for other assets acquired?  | _____ | _____ |
| _____ | 164. Are journal entries prepared that show clearly the nature and purpose of each charge to expense from deferred accounts and evidence of approval by authorized personnel?         | _____ | _____ |
| _____ | 165. Does the association have effective control procedures for all large disbursements to ensure their propriety?  | _____ | _____ |
| _____ | 166. Does the association maintain subsidiary records for the various other asset accounts?   | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

**Deposit Accounts** [120]

- |       |   |       |       |
|-------|---|-------|-------|
| _____ | 167. Is there any limitation on the amount of withdrawal that employees may pay without officer approval?   | _____ | _____ |
|       | If so, what is the amount? _____  |       |       |
| _____ | 168. Are procedures in effect to ensure the timely and accurate completion of the appropriate signature cards upon the opening of deposit accounts?   | _____ | _____ |
| _____ | 169. Does the association segregate duties so that persons opening new certificate accounts do not have sole control over the receipt of cash, account data entry, and the preparation of certificates or receipts? | _____ | _____ |
| _____ | 170. Does the association balance the deposit accounts before and after posting of interest to ascertain correctness of total amount posted?  | _____ | _____ |
| _____ | 171. Does the association maintain general ledger subsidiary accounts for each class of accounts?   | _____ | _____ |
| _____ | 172. Is an analysis made periodically to determine the adequacy of accrued interest earned and unpaid?  | _____ | _____ |
|       | How often? _____  |       |       |
|       | Last as of date? _____  |       |       |
|       | Person responsible? _____   |       |       |
| _____ | 173. Does the person who performs the analysis have an account at the association?  | _____ | _____ |
| _____ | 174. If so, who reviews the account of the person who performs the analysis?  |       |       |
|       | Person responsible? _____   |       |       |
| _____ | 175. Does the association investigate and adjust differences between the accrual balance and the interest paid?   | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

- |       |  |       |       |
|-------|--|-------|-------|
| _____ | 176. Does the association reasonably estimate accruals for reporting purposes?   | _____ | _____ |
| _____ | 177. Are policies in effect to maintain compliance with state escheat laws?  | _____ | _____ |
| _____ | 178. Does the association flag dormant accounts so they can monitor activity?  | _____ | _____ |
| _____ | 179. Does the association waive significant amounts of account fees?   | _____ | _____ |
| _____ | 180. Does the association generate a demand deposit overdraft report?  | _____ | _____ |
| _____ | 181. Does the demand deposit overdraft report identify the name and position of the person(s) responsible for approving overdrafts?  | _____ | _____ |
| _____ | 182. Does the demand deposit overdraft report identify large borrowers and insiders?   | _____ | _____ |
| _____ | 183. Do designated personnel review the demand deposit overdraft reports?  | _____ | _____ |
|       | Person responsible? _____  |       |       |
|       | Approval limits? _____   |       |       |
| _____ | 184. Does the association generate a check-kiting report?  | _____ | _____ |
| _____ | 185. Is the check-kiting report prepared by an individual who does not have an account with the financial association or is the preparer's account independently reviewed? | _____ | _____ |
| _____ | 186. Does the check-kiting report identify insiders and major borrowers?   | _____ | _____ |
| _____ | 187. Is the person responsible for reviewing check-kiting reports independent of the preparation of the reports?   | _____ | _____ |
|       | Person responsible? _____  |       |       |
| _____ | 188. How often does the association review check-kiting reports?   |       | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As Of Date:**>

Verified By Examiner		Yes	No
-------------------------	--	-----	----

**Deferred Credits** [121]

- |       |      |   |       |       |
|-------|------|---|-------|-------|
| _____ | 189. | Does the association maintain records supporting the recognition of profits resulting from the sale of real estate owned? | _____ | _____ |
| _____ | 190. | Does the association maintain records supporting loan acquisition credits deferred and earned, by semiannual periods?     | _____ | _____ |
| _____ | 191. | Does the association amortize loan origination fees in accordance with FASB 91?   | _____ | _____ |

**Other Liabilities** [122]

- |       |      |  |       |       |
|-------|------|--|-------|-------|
| _____ | 192. | Does the association maintain a detailed inventory or subsidiary records for the various other liability accounts? | _____ | _____ |
| _____ | 193. | Does a designated officer make periodic reviews of the activity in other liability accounts?                       | _____ | _____ |
|       |      | Designated officer: _____  |       |       |

**Capital (Reserves, Undivided Profits, etc.)** [123]

- |       |      |   |       |       |
|-------|------|---|-------|-------|
| _____ | 194. | Does management review and the board of directors approve all transfers to and from the capital accounts?     | _____ | _____ |
| _____ | 195. | Does the association clearly explain and adequately document all transactions involving the capital accounts? | _____ | _____ |
| _____ | 196. | Does the corporate officer designated in the bylaws or by the board of directors control stockholder records? | _____ | _____ |
| _____ | 197. | Does the association promptly cancel surrendered stock certificates to prevent their reuse?                   | _____ | _____ |

**INTERNAL CONTROL QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

\_\_\_\_\_ 198. Does an officer designated in the bylaws or by the board of directors sign stock certificates? \_\_\_\_\_

**Letters of Credit** [I24]

\_\_\_\_\_ 199. Does the association have any outstanding unexpired letters of credit? \_\_\_\_\_

\_\_\_\_\_ 200. Has the board of directors adopted a written letter of credit policy? \_\_\_\_\_

\_\_\_\_\_ 201. Does the board review the policy annually and note the review in the minutes? \_\_\_\_\_

\_\_\_\_\_ 202. Does the association maintain a daily transaction journal that summarizes all outstanding letters of credit? \_\_\_\_\_

\_\_\_\_\_ 203. Who is responsible for the preparation and posting of subsidiary records and accounting for fee income?

     Person responsible? \_\_\_\_\_

     Title? \_\_\_\_\_

\_\_\_\_\_ 204. Has the association made commitments on letters of credit that they have not issued and for which the commitment period is unexpired? \_\_\_\_\_

\_\_\_\_\_ 205. Has the association issued any letters of credit on behalf of directors, officers, employees and their interests, or for other insiders? \_\_\_\_\_

     If so, please list: \_\_\_\_\_

\_\_\_\_\_ 206. Has the association issued or confirmed letters of credit to officers or directors of another financial institution? \_\_\_\_\_

\_\_\_\_\_ 207. Does the association's internal loan review process review letters of credit for adequacy of underwriting, documentation, and credit quality? \_\_\_\_\_

\_\_\_\_\_ 208. Are letters of credit of questionable quality listed on the association's problem asset list? \_\_\_\_\_

**INTERNAL CONTROL QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

Verified By Examiner		Yes	No
-------------------------	--	-----	----

\_\_\_\_\_ 209. Has the association had to pay a draft without receiving payment from a customer? \_\_\_\_\_

\_\_\_\_\_ 210. Has the association extended any loans because of letters of credit? \_\_\_\_\_

▾ List all loans extended because of letters of credit:

\_\_\_\_\_

\_\_\_\_\_ 211. Are there any outstanding lawsuits because of letters of credit? \_\_\_\_\_

**Prepared By:** \_\_\_\_\_

**Verified By:** \_\_\_\_\_

**This page intentionally left blank**



**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As of Date:** >

A management official of the association should complete this questionnaire. If the association lacks adequate internal controls regarding funds transfers, the examiner should verify appropriate responses and initial in the verified column. The flagged questions are the suggested minimum verifications. Management must provide the examiner with an adequate written explanation of all "No" answers, with an appropriate reference to the question, and supply copies of applicable written procedures. If a question is not applicable to the association, respond with NA.

	Verified by Examiner		Yes	No	NA
--	-------------------------	--	-----	----	----

***Funds Transfer and Wire Controls***

\_\_\_\_\_ 1. Indicate the method that the association uses to wire funds:

Fedline:

\_\_\_\_\_

Money Transfer Workstation:

\_\_\_\_\_

Voice:

\_\_\_\_\_

\_\_\_\_\_ 2. Average dollar volume and number of transfers:

\_\_\_\_\_

Specify per day, week, month, or other:

\_\_\_\_\_

\_\_\_\_\_ 3. Average daily amount available for transfer, if limited:

\_\_\_\_\_

\_\_\_\_\_ 4. Peak amount available for transfer, if limited:

\_\_\_\_\_

\_\_\_\_\_ 5. Does the association have written wire transfer procedures?

\_\_\_\_\_

**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

	Verified by Examiner		Yes	No	NA
_____		6. Do personnel consistently follow the procedures? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		7. Who is responsible for supervising the wire transfer activity to ensure compliance with the written procedures? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		8. Is an internal or independent audit performed of the wire transfer procedures? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		9. Does the association provide adequate training to personnel involved with the wire transfer process? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		10. Does the association segregate securities-transaction-related duties among the buyer/seller, the trader, and settlement clerk? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		11. Are dual authorizations (maker, approver) required before the sending department acts upon internal wire transfer requests? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		12. Do procedures require that the association actually transfer collected funds out of the customer account before the wire transfer department makes outgoing transfer orders? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		13. Do personnel involved with wire transfers receive proper background screenings, including criminal record investigation? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		14. Are sendable funds limited by using separate correspondent accounts to send and to receive funds? _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**FUNDS TRANSFER QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #:** >

**Institution Name:** >

**Examination As Of Date:** >





	Verified by Examiner		Yes	No	NA
	_____	Are controls to limit daylight overdrafts effective?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		Briefly describe the controls:			
	_____				
	_____	15. Does the association audit the wire transfer log periodically?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	16. Does the association keep a complete log of wire transfer activity for audit?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	17. Does software provide a log of all wire transfer activity?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	18. If a data terminal is used, is an unbroken paper printout copy of all activity reconciled to requests daily?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	19. Are interim daily reconcilements and end-of-day reconcilements performed with all reconciling items cleared?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	20. Does the association prohibit the person who performs end-of-day balancing from executing wire transfers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	21. Is the person who executes wire transfers prohibited from access to cash (such as having a teller drawer)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				
	_____	22. Does the association prohibit the person who reconciles the association's deposit account affected by wire transfer activity from executing wire transfers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	_____				

**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

	Verified by Examiner		Yes	No	NA
_____		23. Is a timely reconciliation made, by a person not involved in the wire transfer process, of wire transfer activity statements from a service provider compared with internal wire transfer activity records?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		24. Does the association keep a permanent record of all customer wire transfers listing the date, amount of the transfer, person authorizing the transfer, test code or PIN, and detailed instructions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
		25. Does the association restrict access to test codes to only those employees authorized to handle wire transfer requests?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		26. Does the association keep the test codes in a secure place?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		27. If the association uses code words, do they change them periodically?  How often?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		28. Does the association strictly forbid the transfer of uncollected funds?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		29. Does the association require dual officer approval for large-dollar transfers?  Who is authorized and what are the limits?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		30. Does the association require customer and/or bank verification callbacks for voice wire transfers above an established dollar threshold?  Who is responsible for verification?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >

**Institution Name:** >

**Examination As Of Date:** >

	Verified by Examiner		Yes	No	NA
_____		31. Does the association make all securities-transaction-related transfers only after the verified receipt of securities (delivery versus payment)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		32. Does a person independent of the transaction approval or processing balance wire transfers at least daily?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		33. Does the association have a dual entry/release system for wire transfers?  For computerized systems, does one person input transfer instructions and another person verify and release the transfer?  For associations that call in wire instructions to a correspondent institution that performs the wire transfer, does one authorized person originate the call; then does the correspondent institution have a second person make a callback to a second authorized person to verify the authenticity of the wire instructions?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		34. Has the association made unusual, frequent, or sizable transfers offshore to Privacy Act Havens (such as Panama, Switzerland, the Netherlands Antilles, or the Cayman Islands)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		35. Does the association require that customer wire-transfer requests be in writing and signed by the customer wiring the funds?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

***Wire Transfers Using Personal Computer Systems***

_____		1. Does the association keep the personal computer executing wire transfers in an area that is physically secure from unauthorized employees and the public?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-------	--	--	--------------------------	--------------------------	--------------------------

**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

	Verified by Examiner		Yes	No	NA
_____	2.	Does each authorized user of the wire transfer system have a unique password known only to that user?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____	3.	Do separate persons enter and release outgoing transfers with separate unique passwords?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____	4.	Do employees adequately protect passwords to ensure that only the authorized user is aware of the password?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____	5.	Does the system require users to change their password periodically?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____	6.	Are procedures (such as the system requiring two users' passwords) in place to ensure that one person enters the wire transfer and another person verifies it before releasing the wire transfer?  ➡ If so, what is the time interval for going into waiting mode?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____	7.	When each user finishes a series of transactions, and leaves the wire transfer terminal unattended, does the terminal go into a waiting mode where it is not possible to send outgoing wire transfers?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Branch Procedures (Customer-Requested Wire Transfers)**

_____	1.	Does a branch procedures manual contain a clear and concise description of branch wire transfer procedures?  _____	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
-------	----	--	--------------------------	--------------------------	--------------------------

**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**

**Institution Name: >**

**Examination As Of Date>**

	Verified by Examiner		Yes	No	NA
_____		2. Are telephone requests from the branch office to the main office for two-party wire transfers accepted?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		3. Briefly, describe the procedures the association uses to ensure that such requests are authentic.			
_____		4. Does the association identify all transfers by sequential code or encrypted passwords in prearranged order with correspondents?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		5. Are third-party wire transfers by telephone confirmed by four-person call-back procedure (sender, receiver, approver, confirmer)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		6. Does the association record all calls?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		7. Does each participant document callbacks?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		Is a signed customer-authorization form required as a source document and proof of authorization for customer-requested wire transfers?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		8. Do the forms indicate the date, time of day, wire-from- and wire-to-account instructions, and initials or signatures of personnel who processed the request?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
_____		9. Does the association retain customer authorization forms?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**FUNDS TRANSFER QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As Of Date>**

	Verified by Examiner		Yes	No	NA
--	-------------------------	--	-----	----	----

***Internally Generated Wire Transfers (Department Requests for Wire Transfers)***

- |       |    |  |                          |                          |                          |
|-------|----|--|--------------------------|--------------------------|--------------------------|
| _____ | 1. | Does the association require that all departmental wire transfer requests be in writing, on a preprinted form?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| _____ | 2. | Does the request form contain all necessary from-account and to-account information?   | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| _____ | 3. | Do departmental request forms indicate the initials or signatures of the initiator and approver who authorized the wire transfer?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| _____ | 4. | Do separate persons originate, approve, and send internally generated wire transfers?  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| _____ | 5. | Do department wire transfer telephone or facsimile requests made from remote locations require a callback to that location to ensure that the wire transfer request actually originated there? | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| _____ | 6. | Does the association have controls in place that require action by two people to complete a transfer, one to receive or initiate the request and another to confirm authenticity?              | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

**Prepared By:** \_\_\_\_\_  
**Verified By:** \_\_\_\_\_



## Information Technology Risks and Controls

This Handbook Section presents the agency's examination guidance and program for assessing information technology (IT) risks in comprehensive examinations of savings associations that do not undergo a separate IT examination. OTS uses this section to evaluate technology risks in an association and assess the strength of an association's internal controls for information technology. The Handbook section focuses on the important control activities of proactive management oversight for information security, business continuity, and vendor management, as well as technology-related audit work.

Technology has revolutionized daily operations in savings associations. Associations have moved away from mainframe-oriented computer processing environments and toward increased reliance on newer technological environments, for example, networks, the Internet, and enterprise-wide processing. This examination guidance reflects these changes. Examiners assess the risks of the association's usage of technology, the overall resulting exposure to technology risks, and the adequacy of controls to mitigate those risks.

---

### LINKS

---

 [Program](#)

If the savings association does not properly identify and mitigate technology risks, there can be serious adverse consequences to its reputation. Examples of technology risks that can substantially damage an association's reputation include unauthorized access to corporate data and customer records, identity theft, inadequate business continuity planning, or fraud. These can also cause significant financial losses to an association. Use this Handbook Section to determine, on a risk-focused basis, whether an association's use of technology is consistent with a safe, sound, and secure operating environment. This Handbook guidance and program complements [Section 340, Internal Controls](#).

## OVERVIEW

Increasingly, associations are using technology to develop and deliver financial products and services, with the goals of improving customer service and reducing operating costs. Even the most traditional, conservative associations have embraced more technology. Associations have made, and continue to make, huge investments in technology to maintain and upgrade their infrastructure, to provide new electronic information-based services, to manage their risk positions and pricing, and to monitor transactions to detect and prevent money laundering and terrorist financing under the Bank Secrecy Act and the PATRIOT Act. At the same time, new electronic products, such as online banking, make it possible for small associations to take advantage of newer technologies at lower costs.

Improved processes, such as automated underwriting and credit scoring, have given borrowers the opportunity to obtain credit cards, mortgages, and small business loans from more financial services providers. Automated underwriting and credit scoring substantially reduce the time and costs involved in making sound credit decisions. These tools have also improved the ability of lenders to evaluate and price credit risk, which allows extensions of credit to a wider range of borrowers. Individuals can easily obtain their credit reports and credit scores and verify the information. They can contact the credit bureau if information in the report is incorrect, and thereby, improve their credit standing.

Information technology has made other significant contributions to associations' profitability. In mortgage lending, credit decisions are made in minutes rather than days and at a much lower cost than a decade ago. New technology has also enhanced competition, making it easier for local associations to offer new products and compete successfully with out-of-market associations. In addition, securitization, which is also highly dependent on advances in information technology, has broadened the pool of mortgage lenders and made the primary and secondary markets far more efficient.

Associations use software and computers in operations due to the volume and complexity of transactions processed each day; in fact, almost every aspect of operations within an association is able to use some technology. Savings associations use technology to develop budgets and business plans, underwrite loans, measure and model interest rate risk, track trust accounts, and monitor suspicious activities; in short, to manage almost every aspect of their operations. As technology evolves, and associations continue to increase their reliance on it, risks increase. The increased risks require effective controls to ensure the integrity, confidentiality, and availability of data.

Risks are inherent in using any technology, and threats to associations come from both internal and external sources. Hackers, disgruntled employees, and errors can adversely affect reliability.

An association's board of directors and management should establish policies, procedures, and controls to ensure confidentiality, integrity and availability of information.

Unauthorized parties might access networked systems that are connected to an association's database, and obtain sensitive, nonpublic customer information. Association websites may be inappropriately altered. Electronic mail containing confidential, proprietary corporate information may be distributed in error.

Clearly, this increased reliance on technology has significantly increased the risks of financial and reputation losses due to unauthorized access to customer and corporate financial records, interruption of services to customers, and fraud. Associations must make choices regarding how to manage and control these risks.

Associations must establish and maintain adequate control systems so management can identify, measure, monitor, and control IT risks that could adversely affect performance or pose safety and soundness concerns. Similar to basic internal controls, associations should design IT risk controls to prevent, to mitigate, and/or to detect and address errors and problems. This process should involve representation from all functional areas, for example, audit, finance, legal, lending, marketing, and IT. These areas should all be involved from the beginning of the process to assess collectively the effects on the association. However, ultimately the board of directors and management are responsible for

developing and implementing the processes, policies, and controls that ensure confidentiality, integrity, and availability for an association's data and systems:

- **Confidentiality:** Customer and corporate information is protected from unauthorized access or use.
- **Integrity:** Information is not altered without permission.
- **Availability:** Authorized users have prompt and continuous access.

The level of technical knowledge required by boards of directors and senior managers varies and is dependent on the size and nature of the association's operations and the degree of complexities within its technology environment. Nonetheless, at a minimum, directors and senior officers should have a clear understanding of the risks posed by technology, provide clear guidance on risk management practices, and take an active oversight role in monitoring risk mitigation activities.

## EXAMINATION OVERSIGHT ACTIVITIES

In conducting risk-focused reviews of information technology in comprehensive examinations, examiners:

- Review the association's IT environment.
- Determine the association's significant technology risks.
- Evaluate management's technology oversight activities, including any technology audit work.
- Assess the strengths of the association's control activities.

You should always consider the level of IT risks and adequacy of the control environment when scoping for examinations and assigning the Management and, as appropriate, the composite CAMELS ratings.

Consistent with a risk-focused approach, you should use judgment in determining the depth of the technology review in comprehensive examinations. The examination work should be consistent with the characteristics, size, complexity, and business activities of the association. To determine the appropriate review, close coordination is needed between the Examiner-in-Charge (EIC), other members of the examination team, and examiners who review the IT risks and controls.

## Examination Coverage

IT examiners review technology risks and controls at associations that have complex operations and activities. Safety and soundness examiners review IT risks and controls during comprehensive examinations, using this examination guidance and its related examination procedures. To supplement

the examination guidance in this Section, we encourage you to refer to the FFIEC IT Examination Handbook Booklets, if necessary.

Regional managers determine whether to assign an IT examiner to review an association's information technology. They consider the most recent information available regarding the association's technology environment and the strength of IT controls. As complexity within an association's technology environment increases, stabilizes, or decreases, examination responsibilities for some associations may move from IT examiners to non-IT examiners.

Factors suggesting an IT examiner may need to review this area include the following:

- Recent, pending, or proposed system conversions.
- Recent or pending mergers and acquisitions.
- Problems and concerns at previous examinations.
- Volume and type of internal processing conducted.
- Complex applications, systems, networks, or equipment.
- Volume of loan servicing.

While these factors suggest a need for an IT examiner, they are not determinative. In scoping, the EIC should consult with the Regional IT Examination Manager regarding IT concerns. Such consultation helps ensure proper evaluation and consistent regulatory treatment.

Significant internal control weaknesses warrant expanded investigation and analysis. In those situations, the examiner completing this program, the EIC, the Regional IT Examination Manager, and the regional Caseload Management team will determine what additional procedures are needed, who should perform them, and whether to conduct them at the current examination or at a future comprehensive or IT examination.

## Information Technology and Management Ratings

The strength of the information technology control environment is one of the factors considered in assigning a rating to the Management component of CAMELS. As stated in [Examination Handbook Section 070](#), the Management component rating must reflect the board's and management's ability and effectiveness in managing all aspects of an association's risks, including the findings and conclusions for IT risks and controls.

The Management rating should always reflect serious control deficiencies for technology risks. Generally, if you identify serious deficiencies with the technology controls, you should rate Management no higher than 2.

*Ratings: IT Concerns*

For examination types 10 and 16, the EIC completes the data field in the OTS Examination Data System (EDS) for the technology examination work. **Note:** This data field is encouraged for examination types 11 and 43, but is not required.

The EIC should select Yes for IT Concerns whenever the exam findings disclose significant IT weaknesses.

This data field prompts the EIC to answer Yes or No to the question:

- Were significant IT concerns noted in the Report of Examination (ROE)?

The EIC should select Yes whenever the examination findings disclose significant IT weaknesses. A significant weakness is one that the EIC concludes is at least partially the cause for lowering the Management rating. A significant weakness could also be something that significantly impacts the association, and management lacks the will or ability to resolve it. If the IT program did not disclose any significant weaknesses, the EIC should answer No.

## Examination Comments and Conclusions

You should incorporate IT examination comments and conclusions into the Management comments, either on the formal report page for Management, or in the Management-related comments summarized under overall Examination Conclusions and Comments. You should present findings under the caption or heading, Information Technology.

Examiners conducting this program assess an association's compliance with the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), 12 CFR Part 570 Appendix B, including Supplement A. The Security Guidelines implement Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act), and Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

The ROE comments should include a brief description of the association's IT environment, significant technology risks, and an overall conclusion as to the adequacy of controls. The report comments should also clearly state whether or not the association is in compliance with the requirements of the Security Guidelines. You must note material instances of noncompliance in the ROE.

You should present significant adverse findings in sufficient detail to identify the specific conditions that require corrective action. Whenever possible, these should include mutually agreeable deadlines for completion of corrective actions. Present corrective actions and deadlines in the Management page comments, or integrate them into the Management-related comments in the Examination Conclusions and Comments. Include significant findings, for example, violations of laws or regulations, on the Matters Requiring Board Attention page.

When examining a state-chartered association, you should also refer to state regulations and follow supplemental regional examination policies and procedures.

## Information Technology Database

OTS developed and maintains the Information Technology Database (IT Database), a national system that provides agency management with information on the thrift industry's data processing activities and technology service providers. The Director, Information Technology Risk Management (ITRM), is the IT Database system owner. ITRM works with OTS Information Systems to maintain and enhance the system, oversee its operations, and update system standards, policies and procedures.

A staff person in ITRM serves as the IT Database National Administrator. In addition to the National Administrator, the regional IT Examination Managers have designated Regional IT Database Administrators. The Regional IT Database Administrators ensure that data collected from the associations, and reviewed by the safety and soundness examiners, are entered into the IT Database, as required.

The IT Database contains information on service providers used by associations, such as names, addresses, significant applications processed, and processing locations, domestic or foreign. The IT Database also collects information about significant applications processed internally by associations. Examiners and Caseload Managers use this information to produce reports that identify technology-related risks, which can be addressed in examinations, off-site monitoring, and other regulatory oversight activities.

The examiner completing the IT procedures collects and reviews the IT Database information for accuracy and completeness, and then provides the information to the regional office for input. The information in the IT Database must be updated every 18 months. If these examination procedures are not conducted within the 18-month timeframe, regional staff must obtain the IT Database information directly from the association.

## INFORMATION TECHNOLOGY ENVIRONMENTS IN ASSOCIATIONS

### Background

Associations have a number of choices available to meet their IT needs. Many OTS-regulated associations outsource a significant amount of their information processing functions to one or more third-party service providers. Others maintain internal data centers to run software licensed from vendors or developed in-house. Mixes or hybrids of these basic approaches are common. An association might contract with one service provider for its general ledger and deposit systems, and with other service providers for loan servicing or its website. Associations also might use licensed software for investments and interest rate risk analysis, and spreadsheets developed in-house for asset quality and board reports.

In addition to outsourcing significant business operations to service providers, most associations are interconnected with various other entities, such as ATM networks and automated clearing houses (ACHs), to process daily business. Associations also maintain one or more internal networks, Local Area Networks, or Wide Area Networks. Each of these arrangements requires a different type and level

of management involvement with regard to data integrity, security measures, and business continuity plans.

OTS expects associations to develop and maintain strong control environments for the information technologies they use. A strong control environment enables management to identify, evaluate, and control risks associated with the business activities. In complex technology environments, it is critical that associations have effective risk management practices and strong internal controls to ensure that all of the technology risks are identified and appropriately addressed. Associations should have effective policies and procedures in place commensurate with the complexity of the IT environment. They also should identify the risks of using technology prior to deploying it, and ensure adequate controls are in place.

## COMPONENTS OF INFORMATION TECHNOLOGY ENVIRONMENTS

### Personal Computers

The personal computer is the most prominent tool in an association's business environment. The power of personal computers has enabled information processing in associations to evolve from the traditional, centralized environment to a decentralized or distributed environment. In addition to its use as a word processor and terminal access device to other computers, a personal computer operates as a powerful standalone computer or within a network of computers. Most associations have at least one internal network, whether it uses third-party service providers, processes internally, or uses a combination of these arrangements.

Using personal computers, association staff can create applications to supplement those provided by third-party service providers or internally operated data centers. For example, staff can use personal computers to originate data, download and manipulate information from an association's databases, and upload the data back into the databases. Each of these activities creates information, which management uses to make decisions that affect business strategies, customer relationships, and regulatory reporting. Management should implement and maintain controls over these activities to ensure confidentiality, integrity, and availability of the information processed and produced.

### Networks

A computer network is an arrangement in which multiple computers are connected to share information, applications, and equipment. By design, networks can increase efficiency, convenience, and access; however, the design also directly affects the specific risks that users must address and control.

Network access can be through a combination of devices such as personal computers, telephones, interactive television equipment, and card devices with imbedded computer chips. The connections are completed principally through telephone lines, cable systems, or wireless technology. It is important to note that not all networks are equally critical, vulnerable, or contain data that is equally sensitive. Every association must evaluate the risks it faces and address those risks.

The Internet is a public network that can be accessed by any computer equipped with a modem. While not centrally managed, the Internet is given order through the World Wide Web (Web), which facilitates visual interfaces and links or electronic connections to other information. The Web also provides multimedia capabilities such as text, graphics, audio, and video.

Intranets are private networks built on the infrastructure and standards of the Internet and the Web. Intranets allow access to databases and electronic documents by defined user groups that are generally limited to internal personnel.

Associations must review and address the security of internal networks, whether private, or configured as local or wide area networks. Internal attacks are potentially more damaging than attacks from outsiders because an association's personnel, who can include consultants as well as employees, have authorized access to critical computer resources. An internal attacker could exploit trusted relationships in networked systems to gain a level of access that allows the attacker to circumvent established security controls. After circumventing the security controls, the attacker could potentially access sensitive customer or corporate information.

Public networks pose additional risks over those of internal networks. Transmitting confidential data over public networks through the use of dedicated or leased lines may provide an inappropriate sense of security. These lines use the infrastructure of public networks; therefore, they are vulnerable to the same attacks as the public networks themselves. Confidential data transmitted via public networks may be intercepted or compromised by individuals for whom the data is not intended. It is therefore important to encrypt sensitive data transmitted via public network infrastructure.

### Local and Wide Area Networks

A local area network (LAN) is a network that interconnects systems within a small geographic area, for example, a building or a floor within a building. Using personal computers or other terminals, users communicate via electronic mail, share printers, and access common systems, databases, and software. A wide area network (WAN) connects users in larger geographic areas. An association might have a LAN within its headquarters, and a WAN for its branches or lending offices to communicate with each other and the headquarters.

LANs and WANs provide substantial benefits in productivity and information access. They facilitate interaction among association staff and between the association and its service providers. Examples of services that associations can offer through their networks include telephone banking, banking by personal computer, ATMs, automatic bill payments, and automated clearinghouse systems for direct deposits or payments. Such access, however, requires that the association apply controls to the personal computers.

Associations that use LAN, WAN, or other network technologies should have policies and procedures that govern purchase and maintenance of hardware and software. Associations must also establish and maintain sound controls that limit access to data and applications based upon job responsibilities, and protect the data's confidentiality and integrity.



## Firewalls

Firewalls are a combination of hardware and/or software placed between networks that regulate traffic that passes through them. They provide protection against unauthorized individuals gaining access to an association's network. Associations should consider firewalls for any system connected to an outside network.

A firewall does not ensure that a system is impenetrable. Firewalls must be configured for specific operating environments and the association must review and update firewall rules regularly to ensure their effectiveness.

## Internet Activities

Association management should have policies, procedures, and controls to govern employee Internet activities. These should address the following:

- Minimizing viruses or other damaging program code associated with downloading files.
- Appropriate use of Internet facilities and services by employees.
- Using encryption to protect sensitive information in transit, for example, electronic mail messages.

## Electronic Banking

Electronic banking is the delivery of information products and services between a customer and an association using electronic access devices such as telephones, automated teller machines, and personal computers. Typically, the devices are connected through a telecommunication line or the Internet.

## Internet Banking

Internet banking refers to the systems that enable customers to access their accounts and information regarding the association's products and services from the association's website via a personal computer or similar communication device.

## Transactional Websites

**Transactional websites**, as defined in CEO Memo 109, allow customers to do any of the following:

- Open an account.
- Access an account.
- Obtain an account balance.

- Transfer funds.
- Process bill payments.
- Apply for or obtain a loan.
- Purchase other authorized products or services.

CEO Memo 109, Transactional Web Sites, states that OTS-regulated associations planning to establish a transactional website must file a Notice with OTS at least 30 days in advance of opening the website to transact business with customers. The examiner conducting the IT examination procedures should determine that the association filed the required Notice with the appropriate regional office.

If the Notice was not timely and properly filed, the EIC should notify the regional caseload management team to determine appropriate remediation. If the Notice was filed pursuant to CEO Memo 109, the examiner reviewing IT risks and controls should contact the regional office to determine if there were any issues that require onsite follow-up review.

Transactional websites also pose specific consumer protection and privacy issues associations should address. See [Handbook Section 1375, Privacy](#), for additional guidance.

Transactional websites that provide for electronic mail between the association and customers require additional controls, for example, encryption, to protect the confidentiality of customer accounts and other sensitive data. Associations should clearly caution customers about sending sensitive data, for example, account numbers, in electronic mail messages to the association or anyone else. For additional guidance see CEO Memo 228, Interagency Guidance on Authentication in an Internet Banking Environment.

### Informational Websites

**Informational websites** provide general information about an association's products and services. Informational websites often highlight loan and deposit programs, branch locations, and operating hours. These may also provide electronic mail addresses for contacting the association and its employees.

Some informational websites provide links to other websites that provide community interest information or other related product information. Thrift Bulletin 83 provides guidance regarding these web-linking arrangements.

## CONTROL ACTIVITIES FOR INFORMATION TECHNOLOGY RISKS MANAGEMENT OVERSIGHT

### Responsibilities of the Board of Directors

Boards of directors have the ultimate responsibility for all technology deployed in their associations. They should approve their associations' overall business and technology strategies. The board of directors and management cannot delegate responsibility for technology controls to service providers, software vendors, or even internal staff. The board of directors must ensure that strong controls for technology risks exist throughout the association.

The level of knowledge required by boards of directors and management is dependent on the size and nature of an association's operations and the degree of complexity within its technology environment. Nevertheless, association directors and management should have a clear understanding of the risks posed by using specific technology, provide clear guidance on risk management practices, and take a proactive role in overseeing technology risk mitigation activities. An association's board of directors and management must effectively plan for using technology, establish a strong control environment, including audit or other independent review of the controls, and educate and support the association's technology users.

To manage effectively the risks associated with complex technology environments, some associations have established a senior management Information Technology committee. This committee is responsible for overseeing the relevant technology control functions throughout the association, for example, in the auditing, legal, and financial divisions, and ensuring these controls are integrated into a framework of risk management for information technology. This senior management committee regularly reviews new products and activities and provides final approval of transactions. Such senior management committees can serve as an important part of an effective information technology control infrastructure.

### Strategic Planning for Information Technology

Deficiencies in planning for deploying technology significantly increase the risks posed to an association and its ability to respond effectively. Therefore, regardless of asset size, associations should have an appropriate plan for technology that outlines the framework for the uses of technology. The substance and form of such a plan will vary from association to association and be dependent on the complexity of the association's operations. The key elements are whether and how well the technology planning process meets the association's needs.

Associations should update their technology plans annually. A satisfactory technology plan coordinates the technology initiatives and activities to the overall business planning process. It should also address the technology strategy used, for example, a combination of internal and outsourced processing that supports delivery of the selected products and services.

Associations intending to implement a transactional website should address this in the technology plan. Management should consider the implications of a transactional website on the association's long-term goals and strategies, and obtain input from the affected business line and technology managers. Planning for a transactional website should address the required advance notice to OTS and include a thorough review of the risks posed by a transactional website to information security, business continuity, and vendor management.

### Training Information Technology Users

Associations must properly educate and support employees and customers to achieve user acceptance of, and confidence in, the association's information systems and technology. Associations should provide training to employees and customers to use applications properly. Associations must also support users with prompt responses to problems. If an association fails to provide reasonable training and support for customers and staff, commitment to the system and its applications deteriorates, administrative costs increase, and avoidable errors may occur. Training deficiencies also raise the risk of data integrity problems and potential for complaints.

Associations should fully inform staff of any changes or updates to systems. Associations should also train staff on how to respond to and execute the business continuity plan. If the association chooses to outsource this function, it must carefully evaluate the third-party vendor's qualifications prior to signing any contracts. Management should also provide backup training for key job functions.

For additional guidance on Management control activities, see [Examination Handbook Sections 310, Oversight by the Board of Directors](#), and [330, Management Assessment](#), and CEO Memo 201, FFIEC IT Examination Handbook, Management Booklet.

## AUDITS AND OTHER INDEPENDENT REVIEWS

All associations should adopt and maintain an audit program. An effective audit function is essential to an association's safe and sound operations. It provides the framework for assessing the effectiveness of the association's risk management practices. It also facilitates reporting to the board of directors and management on the strengths and weaknesses within the association's internal controls. To ensure adequate audit coverage, associations may use internal audit work, external audit work, or a combination of both depending on the association's audit risk assessment. Effective audit coverage substantially improves an association's ability to detect potentially serious problems.

The audit work may be completed internally or externally, however, someone that is qualified and independent of the process or function reviewed must complete the work. This independent person can conduct the audit work separately, as an audit of a specific technology activity, or incorporate it into the audit work for a specific operating department or business line.

The complexity of financial products, services, and delivery channels makes the inclusion of risk-based IT audit coverage an important consideration in establishing an effective overall audit program. Effective audit coverage of technology risks requires personnel that have the skills and experience to identify and report on compliance with the association's policies and procedures. These skills and

experience should include strong abilities to understand technology risks, as well as a detailed understanding of the association's IT policies and procedures.

Audit procedures are most effective when designed into the technology or system during development. When combined with a strong risk management program, a comprehensive, ongoing audit program allows the association to protect its interests and those of customers. In developing an audit program for technology, an association should consider how each application protects fully the financial and informational assets, system reliability and availability, and user confidence.

See Thrift Bulletin 81, Interagency Policy Statement on the Internal Audit Function and Outsourcing, for additional guidance on OTS expectations for an internal audit program.

### Technology Audit Plan

An association's audit plan should provide for reviewing its technology risks. It is the responsibility of the board of directors and management to determine how much auditing will effectively monitor the internal control system, taking into account the audit function's costs and benefits. For associations that are large or have complex operations, the benefits derived from a full-time manager of audit or an auditing staff will likely outweigh the costs. For small associations with few employees and less complex operations, these costs may outweigh the benefits. Nevertheless, even a small association without an internal auditor can ensure it maintains an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls.

Generally, a technology audit will:

- Review technology policies, standards, and procedures.
- Assess how technology affects association operations.
- Determine if technology activities are consistent with management policies and procedures.
- Substantiate the integrity of employee activities and appropriateness of user access rights.

Audit work for technology should validate that all the business lines are complying with the association's standards for technology usage, and appropriately identify any exceptions. This validation should include transaction testing that confirms policy compliance, existence of proper approvals, adequacy of documentation, and integrity of management reporting.

Technology audit work should have clear procedures for when and how to expand the scope of audit activities. There should also be procedures for reporting audit findings directly to the association's board of directors or audit committee, as well as management in the audited area. Associations should implement follow-up procedures to ensure that management resolved all audit findings satisfactorily and the business unit or department implemented audit recommendations in a timely manner.

The complexity of the association's technology environment may cause some associations to retain outside consultants, accountants, or lawyers to review this area. The retention of independent expertise may be an effective method to control effectively the overall risk. For example, associations may employ external auditors to test the technology environment and ensure compliance with policies and procedures. The resulting reports can provide valuable insight to the association in improving its risk controls and oversight.

Additional guidance regarding External and Internal Audit is found in Handbook Sections [350](#) and [355](#), and CEO Memo 182, FFIEC IT Examination Handbook, Audit Booklet.

## INFORMATION SECURITY RISKS AND CONTROLS

An association's corporate data and customer information must be available, accurate, complete, valid, and secure. Information security is the process or methodology an association uses to protect its corporate and customer information. Strong and effective information security is essential to an association's safety and soundness, and should be commensurate with the complexity of its operations and IT environment. The most effective information security has strong board of directors and management support and controls implemented throughout the association's business operations.

Effective information security is not a judgment or conclusion about the condition of IT controls at a particular point in time. Rather, effective information security is an ongoing and evolving process. An association has effective information security when it successfully integrates its processes, people, and technology to mitigate risks to acceptable levels in accordance with its risk assessment. OTS expects an association's information security program will have an incident response component for responding to specific risks, for example, unauthorized access attempts. The information security program should also provide for regular testing as well as security training of employees and other users.

An effective information security program serves as the overall framework that identifies risks, develops and implements a security strategy, tests key controls, and monitors the risk environment. This framework stresses the important roles of senior management and boards of directors by emphasizing their responsibility to recognize security risks in their associations and effectively mitigate security risks by assigning appropriate roles and responsibilities to management and employees.

The scope of an association's information security program should address all technology activities, for example, personal computers, Internet-based banking, and processing by the association's service providers. Effective security does not rely on one solution; rather it requires several measures, which, taken together, serve to identify, monitor, control, and mitigate potential risks to that information. Associations should use several differing controls to manage and ensure information security. Among these commonly found in associations are controls for authentication, passwords, user identification (ID), user access, system log-on and log-off, virus protection, and encryption.

## Information Security Controls

### Authentication

Savings associations use authentication controls to verify and recognize the identity of parties to a transaction. Typically, such controls include computerized logs, digital signatures, edit checks, and separation of duties. Weak authentication controls can allow the accuracy and reliability of data to be compromised from unauthorized access and fraud, errors introduced into the systems, or corruption of data and information. Associations should use effective authentication controls to restrict access and preserve integrity of data.

Authentication procedures for access to sensitive data minimally require a password. Maintenance procedures should ensure that only the user has knowledge of the user's password. Associations should have procedures that allow only users to change their own passwords. Password controls should have all of the following:

- Length of at least six characters, preferably more.
- A mixture of alphabetic, numeric, or other characters.
- Expiration dates that require users to change passwords frequently.
- Restrictions on reuse of previous passwords.
- Automatic lockouts after a defined number of failed log-on attempts.
- Suppression over the display of user passwords in any form.
- Encryption of password files.

On October 12, 2005, OTS and the other federal financial regulators issued updated guidance on risks and risk management controls to authenticate identity of customers accessing an association's Internet-based financial services. This guidance, distributed in CEO Memo 228, Authentication in an Internet Banking Environment, addresses the increased risks to associations and their customers from the growth of Internet banking and other electronic financial services, and the increased incidents of identity theft and fraud. As this guidance relates, associations need effective authentication systems to comply with requirements for safeguarding customer information, prevent money laundering and terrorist financing, and reduce fraud and theft of sensitive customer information.

The level of authentication an association uses should be commensurate with the risks of the Internet-based products and services offered. Associations should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where an association's risk assessment indicates the use of single-factor authentication – only a log-on ID or password – is inadequate, the association should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate these risks. OTS considers single-factor authentication

inadequate as the only control mechanism for higher-risk transactions involving access to customer information or movement of funds to others.

OTS expects associations to achieve substantial compliance with the authentication guidance distributed in CEO Memo 228 by December 31, 2006.

### User Access Rights and Controls

Associations should also establish controls to limit user access. For example, associations should limit access to the Security Administrator account to the smallest number of persons practical without adversely affecting operations. Security Administrators should not have access to customer records. In addition, the association may grant contractors and consultants access to an association's systems. The association should tightly control these access rights.

Access rights to a system enable transaction processing and information retrieval. For outsourced systems, service providers typically set up generic access profiles for common job categories, for example, teller profiles. Associations should not accept and use the vendor access profiles without reviewing them. This increases the risk of inappropriate user access and weakens the control environment for sensitive data. To ensure user access is appropriate, associations should:

- Assign job responsibilities to provide for segregation of duties and dual control.
- Assign user retrieval and information processing capability profiles, based on job responsibilities.
- Ensure separate access profiles for their different systems.

User identification controls should require:

- Management approval to issue a new user ID.
- A unique user ID for each user. Multiple users should not be assigned to one user ID unless there are mitigating controls.
- Restrictions on issuing multiple identifications unless there are mitigating controls.
- Effective procedures to delete, disable, or change access rights promptly for terminated or reassigned employees.

Inappropriate user access assignments could be caused by control deficiencies in granting these rights or by weaknesses in the system security controls. System security control weaknesses can result from software rules that permit inappropriate grouping of user access rights. Weaknesses also arise when software capabilities are not properly invoked. Not enabling the supervisory override capability over dormant accounts is an example of such a weakness.



Management should periodically conduct independent reviews of user access rights to ensure user access assignments are appropriate and properly controlled. Management should document the findings of these reviews and resolution of any recommendations. Regardless of the cause, you should comment in the ROE on inappropriate user access rights.

## Other Information Security Controls

System log-on and log-off controls should limit the number of unsuccessful log-on attempts to a user account. Associations should consider a control that notifies users of unsuccessful attempts since the user's last log-on. Associations should also require that personal computers and system access terminals automatically log-off after a brief period of inactivity.

Associations should install virus protection software on all personal computers and servers to prevent corruption of data or systems. Virus protection controls should include both association policies and installed software. An association's policies should restrict employees from adding software to their personal computers. The policy should also provide for periodic review or audit of the employees' personal computers to ensure conformance with association policies. Anti-virus software should be updated regularly to protect against new viruses.

Acknowledgement controls, such as batch totaling, sequential numbering, and one-for-one checking against a control file, verify proper completion of electronic transactions. For example, if an electronic transmission is interrupted, the association should have controls in place to notify the sender of the incomplete transaction and prevent duplication during re-submission.

Encryption technology scrambles data and information so it cannot be read or understood without the proper codes for unscrambling. Confidential or sensitive data and information in transit should always be encrypted. This includes email containing confidential or sensitive information, as well as Internet banking transactions. As part of performing its risk assessment, association management should identify the strength of encryption needed for specific categories of information.

For additional guidance regarding information security, see CEO Memo 172, FFIEC IT Examination Handbook, Information Security Booklet. This booklet will be updated and reissued in 2006.

## INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

### 12 CFR Part 570 Appendix B and Supplement A Security Guidelines and Association Responsibilities

The Interagency Guidelines Establishing Information Security Standards implement:

- Section 501(b) of the GLB Act, which requires the federal financial regulators, including OTS, to establish standards for administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity, and proper disposal of customer information.
- Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which requires the federal financial regulators to issue regulations directing associations to ensure the proper disposal of consumer information. See [Examination Handbook Section 1300, Fair Credit Reporting Act](#), for guidance on the FACT Act.

For additional guidance on an association's compliance obligations for the Security Guidelines, see CEO Memo 231, Compliance Guide for the Interagency Guidelines Establishing Information Security Standards.

### Differences Between Security Guidelines and Privacy Rule

The requirements of the Security Guidelines, 12 CFR Part 570 Appendix B and Supplement A, and the Privacy Rule, 12 CFR Part 573, both relate to confidentiality of customer information. However, they have different focuses:

- The Security Guidelines address safeguarding confidentiality and security of a customer's information and ensuring proper disposal. The focus of the Security Guidelines is preventing or responding to foreseeable threats against, or unauthorized access or use of, that information. Further, the Security Guidelines state that associations must contractually require their service providers that have access to customer information to protect that information.
- The Privacy Rule limits disclosure of nonpublic personal information. The Privacy Rule prohibits disclosure of a consumer's nonpublic personal information unless certain notice requirements are satisfied and the consumer does not elect to opt out of the disclosure. The Privacy Rule does not impose any obligations with respect to safeguarding information. The Privacy Rule only requires associations to provide privacy notices to customers and consumers that describe their policies and practices to protect the confidentiality and security of nonpublic personal information.

### Role of Board of Directors

The Security Guidelines require the association's board of directors, or an appropriate committee of the board, to develop, implement, and maintain a written information security program. Initially, the board or a committee must approve the written information security program. Thereafter, the board, or an appropriate committee, must oversee implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing reports prepared by management. Management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and the association's compliance with the Security Guidelines.

An association's board of directors is responsible for developing, implementing, and maintaining a written information security program.

Thereafter, the board, or an appropriate committee, must oversee implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing reports prepared by management. Management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and the association's compliance with the Security Guidelines.

### Information Security Program

Under the Security Guidelines, each association must develop and maintain an effective written information security program tailored to the complexity of its operations. Associations must identify and evaluate risks to its customers' information, including the risk of improper disposal of customer and consumer information. An association must also develop plans to mitigate these risks and implement appropriate controls, including proactive oversight and monitoring of its service providers that have access to the association's customer information.

Additionally, the Security Guidelines require that associations test, monitor, and update the information security program, as needed. Management should report the status of the information security program to the board of directors at least annually. The reports should discuss material issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

### Objectives

As detailed in the Security Guidelines, the objectives of a written information security program are:

- Security and confidentiality of customer information.
- Protection against anticipated threats or hazards to the security or integrity of customer information.
- Protection against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.
- Proper disposal of customer and consumer information.

### Risk Assessment

A written information security program begins with conducting an assessment of the reasonably foreseeable risks. Like the other elements of its information security program, the association's risk assessment should be documented. The Security Guidelines recommend the following steps in conducting a satisfactory risk assessment:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.
- Assessing the likelihood and potential damage of the identified threats, taking into consideration the sensitivity of customer information.
- Evaluating the sufficiency of the policies, procedures, customer information systems, and other arrangements an association has in place to control risks identified.
- Applying the preceding three steps in connection with disposal of customer information.

For additional guidance regarding conducting an information security risk assessment, see the FFIEC IT Examination Handbook, Information Security Booklet.

### Managing and Controlling Risk

Managing and controlling information security risk is an ongoing process. An association should review its policies and procedures on an ongoing basis to ensure they are adequate to safeguard customer information and customer information systems, and to ensure proper disposal of customer and consumer information. The association should include the review and findings in reports on the written information security program. The association should also update its risk assessment for new products and services and before implementing system changes.

The Security Guidelines provide a list of control measures associations must consider and adopt, as appropriate. For example, an association must consider controls to restrict access to sensitive or nonpublic customer information. These controls should restrict access only to individuals who have a need to know such information. Associations must also consider whether encryption of customer information maintained in electronic form is warranted in light of its information risk assessment. If so, the association should adopt appropriate encryption measures to protect information in transit, storage, or both.

Associations should train staff to implement and maintain the written information security program. Associations should provide specialized training to ensure personnel protect customer information in accordance with requirements of the information security program. For example, they should train staff to recognize and respond to attempted fraud and identify theft, guard against pretext calling, and dispose properly of customer and consumer information.

Associations also should test key controls, systems, and procedures of the information security program. The association's risk assessment should determine the scope, sequence, and frequency of testing. OTS expects testing to be done periodically at a frequency that takes into account the rapid evolution of threats to information security. Independent third parties or staff other than those who develop and maintain the information security program should perform and review the testing.

An association should adjust its written information security program to reflect the results of the ongoing risk assessment and key controls. An association should adjust the program to take into account changes in technology; the sensitivity of customer information maintained; internal or external threats to information; and its own changing business arrangements, such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

### Security Guidelines and Service Providers

The Security Guidelines have specific requirements that apply to service providers. In addition to exercising due diligence in selecting a service provider, an association must enter into and enforce a contract that requires the service provider to implement appropriate measures designed to meet the objectives of the Security Guidelines. The contract guidance in the Security Guidelines applies to all service providers, affiliated and nonaffiliated.

Consistent with OTS and interagency outsourcing guidance, the Security Guidelines also require an association to monitor its service providers to confirm they satisfy all contractual obligations to the association. Among other things, these obligations include protecting against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer, and proper disposal of customer and consumer information.

The Security Guidelines do not impose specific requirements regarding methods used or frequency of monitoring service providers to ensure they are fulfilling their obligations under contracts. An association must monitor each service provider in accordance with its risk assessment for potential risks posed by the service provider. These activities could include reviewing audits or summaries of test results conducted by a qualified party independent of management and personnel responsible for development and maintenance of the service provider's security program. An association should document its reviews of service providers in the written information security program.

### Security Guidelines and Disposal Rule

The Security Guidelines direct associations to require in contracts that their service providers implement appropriate measures designed to meet the obligations of the guidelines regarding the proper disposal of consumer information. Although the Security Guidelines do not prescribe a specific method of disposal, OTS expects associations to have appropriate risk-based disposal procedures for records. As indicated in their risk assessments, associations should ensure that paper records containing customer or consumer information are rendered unreadable. Associations should also recognize that computer-based records present unique disposal problems.

The Security Guidelines required associations to satisfy the disposal guidelines by July 1, 2005, and to modify affected contracts with service providers by July 1, 2006.

## Supplement A to 12 CFR Part 570 Appendix B

### *Incident Response Program*

On March 29, 2005, OTS and the other federal financial regulators issued guidance regarding programs to respond to unauthorized access to customer information and when to provide customer notice (Incident Response Guidance). According to this guidance, an association should develop and implement a response program to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The components of an effective response program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused.
- Prompt notification to OTS once an association becomes aware of an incident involving unauthorized access to or use of sensitive customer information.
- Notification to appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate action.
- Filing a timely Suspicious Activity Report, consistent with OTS regulations and instructions.
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence.
- Notification to customers, when warranted.

### *Customer Notification*

The Incident Response Guidance describes when and how associations should provide notice to customers affected by unauthorized access or misuse of their information. In particular, once an association becomes aware of an incident of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine the likelihood the information has been or will be misused. If it determines that misuse of customer information has occurred, or is reasonably possible, the association should notify the affected customer as soon as possible.

Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a PIN or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow an

unauthorized third party to log onto or access the customer's account electronically, such as user name and password or password and account number.

The Incident Response Guidance also states that an association's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to customer information, including notification to the association as soon as possible following any incident. For additional guidance on response programs for security breaches and notifying affected customers, see CEO Memo 214, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

If OTS finds an association's performance is deficient under the Security Guidelines, it may take appropriate corrective action. The agency could require the association to file a compliance plan in accordance with the regulations implementing the Prompt Corrective Action provisions of the Federal Deposit Insurance Act. Or, OTS could initiate an enforcement action under 12 CFR § 568.5 for noncompliance with the Security Guidelines.

## BUSINESS CONTINUITY RISKS AND CONTROLS

### Board of Directors and Management Responsibilities

Associations must be capable of restoring critical information systems, operations, and services quickly after an adverse event. Effective business continuity planning can ensure associations are prepared to respond to events such as natural disasters, human error, terrorist activities, or a pandemic. For additional guidance on preparations for a pandemic, see CEO Memo 237, Interagency Advisory on Influenza Pandemic Preparedness.

The board of directors is responsible for developing and annually reviewing test results and approving the association's Business Continuity Plan.

An association's board of directors and management are responsible for all of the following:

- Establishing policies and procedures, and assigning responsibilities to ensure that comprehensive business continuity planning, including testing, takes place.
- Annually reviewing the adequacy of the association's business continuity plan and test results.
- Documenting such reviews and approval in the board minutes.
- Evaluating adequacy of contingency planning and testing by service providers.
- Ensuring that the association's business continuity plan is compatible with that of its service providers.

Business continuity plans can minimize disruptions caused by problems that impair or even destroy the association's processing and delivery systems. Extended disruptions to the association's business operations pose substantial risks of financial losses, and could lead to the failure of an association. Effective business continuity planning requires a comprehensive, association-wide approach, not a narrow focus on recovery of the association's systems and technology.

### Business Continuity Planning Process

Business continuity planning is the process of reviewing all of an association's departments and business lines and assessing the importance of each to the association and its customers. Association management then develops and maintains a written business continuity plan that addresses all significant products and services, and the outsourced and internally operated information systems and technology that support these.

The complexity of an association's IT environment should dictate the level of detail contained in the business continuity plan. As the association adds new information systems and technology to its environment, it should revise the business continuity plan. The beginning point should be a business impact analysis. This assesses the risks posed to each system, and then identifies the principal departments, resources, activities, and users potentially affected by a problem. This includes assessing the response capability of the association, the alternate processing site, transportation and storage of backup media, and third-party vendors who can provide alternate processing locations.

If the association has contracted with a third-party vendor, management must obtain, review and determine adequacy of the service provider's business continuity plan and testing. The vendor's plan should be compatible with, and integrated into, the association's business continuity plan. However, merely maintaining the vendor's business continuity plan, and participating in its periodic connectivity testing, is not adequate to satisfy this requirement. An association must have its own business recovery and continuity plan specifically designed for its operating profile and IT environment.

### Business Continuity Plan Development

A business continuity plan should define the roles and responsibilities for recovery team members. The detail will vary among associations, depending on the degree of risk inherent in operations, the level and complexity of information technology used, and the association's available resources. However, the business continuity plan should be in sufficient detail so an association can respond effectively to a problem situation.

Typically, an association's business continuity plan should:

- Designate the individual(s) responsible for coordinating all activities in responding to a disaster when the business continuity plan is invoked.
- Define roles and responsibilities for each team member.



- State clearly how potential disasters could affect the association's departments, products, services, employees, and customers.
- Provide details on potential risks and describe strategies, resources, and procedures for recovery.
- Establish the periodic frequency for testing and ongoing training of employees.
- Specify a clear timeline for recovering significant operations.

A clear timeline for recovery is critical to the business continuity plan. Recovery does not mean when an affected system becomes available again. In achieving full recovery, the association may have to correct or resubmit transactions that were in process when the disaster or disruption occurred. This could involve a full day's transactions or more.

Additionally, an association's business continuity plan should address the differing requirements posed by outsourced and internally operated systems. For outsourced systems, the association's business continuity plan should address the following for each significant service provider:

- Categories and sources of data input, for example, branch transactions entered by personal computers or terminals.
- Work steps or processes to recover for resubmission data previously input.

For each internally operated system, the association's business continuity plan should address:

- Recovery of lost data, for example, day-of-disaster online input.
- Replacement of damaged hardware and software resources.
- Alternate processing locations.

### Business Continuity Plan Monitoring and Testing

An association should test its business continuity plan at least annually. Acceptable testing methodologies include tabletop drills, walk-through exercises, and simulations. An association should modify its business continuity plan to reflect testing results and any changes to the association's information systems and technology environment.

The association's business continuity plan should also designate an incident response team. Generally this team would consist of a small number of staff from the departments and functions designated as critical to recovery of operations. Collectively, the team provides the resources necessary to respond quickly and decisively to problems.

For additional guidance on business continuity planning, see CEO Memo 176, FFIEC IT Examination Handbook, Business Continuity Planning Booklet.

## VENDOR MANAGEMENT RISKS AND CONTROLS

Associations use outsourcing to reduce costs and achieve strategic goals more efficiently. More and more, associations use third parties to conduct business operations associations previously conducted directly. Given current technology environments, these outsourcing arrangements are becoming increasingly complex, and may involve foreign-based entities. **Note:** Outsourcing is use of a third party, either affiliated or nonaffiliated, to perform activities on a continuing basis, that the association would normally handle.

An association's board of directors and management should develop and approve policies for overseeing its service providers.

Outsourcing can be the initial transfer of an activity or function from the association to a third party, or from the original third party to another third-party service provider, which is sometimes referred to as subcontracting. Another major trend in outsourcing is offshore outsourcing or moving processing activities outside the United States.

Offshore outsourcing introduces country risk for associations. In offshore outsourcing, associations must also monitor foreign government policies, and political, social, economic, and legal conditions in the country where it has a contractual relation with the service provider. Because of this, an association should develop appropriate contingency plans and an exit strategy for foreign outsourcing relationships. The association should have a strategy to transfer the processing activities back to the United States should it become necessary.

Examples of commonly outsourced operations include accounting, human resources administration, and customer call centers. Associations may also determine that use of a specific technology is too sophisticated or dynamic to be supported effectively within the association. These associations may determine that some or all of such technology should be outsourced to a third-party vendor.

As stated in Thrift Bulletin 82a, Third Party Arrangements, the Home Owners' Loan Act (HOLA) requires associations to notify OTS of arrangements with all third-party providers. HOLA requires such notice regardless of whether or not there is a contract. Generally, associations must provide notice to a Regional Director, for both domestic and foreign third-party arrangements, within 30 days after the earlier of:

- The date the association enters into the contract with the third party.
- The date the third party initiates performing the services.

### Service Provider Due Diligence

The association must also conduct adequate due diligence in selecting its service providers. Prior to the formal selection, it should develop specific criteria to assess a third-party service provider's capacity and ability to perform the outsourced activities effectively. Appropriate due diligence includes selecting those service providers that are qualified and have adequate resources to perform the work. It also involves ensuring the service provider understands and can meet the association's requirements. It is also important that an association verifies the service provider's financial soundness to fulfill its obligations.

Prior to outsourcing any aspect of its operations, the association should establish specific policies and procedures. Management should demonstrate a comprehensive understanding of outsourcing's expected benefits and costs. Management also should develop and implement a formal program to monitor the service provider relationship. A comprehensive vendor management oversight program should provide for ongoing monitoring and controlling of all relevant aspects of the service provider relationship.

If a service provider fails, or is otherwise unable to perform the outsourced activities, it may be costly and problematic to find alternative solutions. The association should consider transition costs and potential business disruptions. An association should not outsource activities to a service provider that does not meet all of an association's due diligence criteria.

### Service Provider Contracts

A clearly written contract should govern all outsourcing arrangements. Associations can mitigate outsourcing risks by carefully negotiating and reviewing service provider contracts, including contract renewals, prior to signing. Legal counsel should always review the vendor contracts to determine that the association's interests are adequately protected. Associations should actively monitor vendor performance, and verify performance level reports periodically.

Key contract provisions should:

- Define clearly outsourced activities and expected service and performance levels.
- Provide for continuous monitoring and assessment of the service provider so the association can take timely corrective action.
- Include a termination clause and time period or conditions under which it would be exercised.
- Address issues related to subcontracting for all or part of the outsourced activity.
- Cover requirements detailed in the Security Guidelines that are contained in the association's written information security program.

### Service Provider Management and Monitoring

Typically, the association forwards data to the service provider's processing center, usually via on-line data entry terminals; output reports are available at the association's on-line terminals and printers. For those portions of the service provider's systems that are within the association, the association has responsibility for establishing and maintaining appropriate controls. For example, an association should develop controls that restrict access to teller terminals to tellers and other specifically authorized personnel. An association should also develop controls for balancing and reconciling items processed by the third-party vendor. The contract should address these responsibilities.

An association that is part of a holding company structure may have an affiliated company provide its technology needs. The affiliated service provider could be a department within the parent holding company, or a separate affiliate of the association. This type of arrangement typically reduces costs and achieves enterprise-wide economies of scale. However, contracts among affiliated entities may raise supervisory concerns. See the Holding Company Handbook for additional guidance on transactions with affiliates.

Vendor contracts should specify performance measures; two key metrics are online up time and terminal response time. Up time refers to the hours and days online services will be available. Often, these are the hours the association's branches operate, plus two or three additional hours daily. Contracts should state the vendor's performance commitment, for example, 99 percent up time. Terminal response time refers to the customary elapsed time between transaction initiation, when the enter key is pressed, and delivery of information to the screen. Response time should be measured in seconds.

Service provider contracts should also address non-production or non-processing products and services. Examples of these are audited financial statements for the vendor, third-party audits of the service provider, or summaries of the vendor's disaster recovery testing results. An association should obtain and review these as part of a proactive vendor management program.

An association should obtain IT ROEs for its significant service providers. An association should also obtain third-party reviews of its significant service providers. A third-party review is an independent evaluation the service provider obtains to meet the needs of client associations. A qualified auditor who is independent of the service provider conducts the third-party review. The scope of this audit should be broad enough to satisfy the audit objectives of the service provider and the client associations.

The American Institute of Certified Public Accountants' Statement of Auditing Standards 70 (SAS 70) provides guidance for auditors performing the service provider review and to auditors of client financial associations. The SAS 70 reviews should determine the adequacy of controls in areas such as the service provider's data center, systems and programming, and input/output controls. The controls reviewed at the service providers should have reciprocal controls at the individual client associations. In the SAS 70 review, the auditor will address these corresponding controls, in a section typically referred to as "client control considerations." An association should obtain and review these reports, and take appropriate actions for any client control considerations or weaknesses discussed. It is also important that an

association understand the scope of the SAS 70 review to determine if it adequately assesses all relevant control areas.

For additional guidance on vendor management oversight activities, see Thrift Bulletin 82a, Third Party Arrangements, and CEO Memo 201, FFIEC IT Examination Handbook Outsourcing Technology Services Booklet.

## OTHER ASSOCIATION CONTROLS FOR INFORMATION TECHNOLOGY RISKS

### Input and Output Controls

An association should require additional controls for technology used to process information, which has direct monetary effects on either the association or its customers. These controls should include requirements that there be segregation of duties between input of information and review of that information post-processing. Such controls should also require the post-processing reviewer to reconcile the processed information.

For large dollar transactions, for example, funds transfers, associations should require that all phases of the transaction be performed under dual controls. For mortgage loan set-ups, verification procedures should consist of manually comparing a sample of source documents against system reports. The association's written policies and procedures should describe these controls in full detail.

### Change Control Management

An association must prepare to adapt activities and information technology to meet changing requirements and circumstances. Association management should ensure that changes to existing technology undergo the same due diligence as new technology selections. An important consideration in technology changes is that there be thorough testing. Additionally, an association should maintain accurate and complete records describing the changes, reasons for the changes, and those responsible for making them.

### Conversion Project Management

Any association that uses IT to perform operations or provide services must commit to update continuously its activities to keep current with technological changes. For example, if an association experiences a corporate merger or acquisition, wants to reduce or more effectively control costs, or offer new products or services, it must plan to convert its operations and systems to accommodate these changes.

In highly technological environments, it is likely that an association will experience at least one or more systems conversion. A systems conversion is the process of replacing existing applications with new ones developed internally, or with third-party vendor software through an outsourcing agreement. The association should conduct planning, testing, and monitoring of new activities as part of its risk mitigation processes.

A conversion presents significant risks to an association, which can be mitigated with adequate project management controls. Flawed or failed conversions are very costly, and can compromise the integrity and reliability of books and records, causing unsafe and unsound conditions within the association. For example, in a flawed check processing conversion, an association could be forced to charge-off significant, unresolved bookkeeping differences. In a flawed deposit conversion, management could have unreconciled deposits requiring adjustments and write-offs. These can cause significant financial losses and waste management resources.

The board of directors should monitor planning and implementation of major system conversions. The directors should also hold management accountable for the success or failure of these conversions. Management should develop and oversee the successful completion of tasks and milestones by both the vendor and association personnel. User testing, debugging, and staff and customer training should occur before implementation or conversion of any system.

## REGULATORY GUIDANCE AND REFERENCES

### Code of Federal Regulations (12 CFR)

§ 555	Electronic Operations
§ 563.161	Management and Financial Policies
§ 563.170	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 568	Security Procedures
Part 570	Safety and Soundness Guidelines and Compliance Procedures
Appendix A Part 570	Interagency Guidelines Establishing Standards for Safety and Soundness
Appendix B Part 570	Interagency Guidelines Establishing Standards for Information Security
Supplement A	Interagency Guidance on Response Programs for Unauthorized Access to Customer
Appendix B Part 570	Information and Customer Notice

## Office of Thrift Supervision Guidance

*CEO Memoranda*

- No. 109                    Transactional Web Sites
- No. 139                    Identity Theft and Pretext Calling
- No. 172                    Information Technology Examination Handbook – Information Security Booklet
- No. 176                    Information Technology Examination Handbook – Supervision of Technology Service Providers and Business Continuity Planning Booklet
- No. 179                    Request for Comment on Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- No. 182                    FFIEC Information Technology Examination Handbook – Audit Booklet, FedLine Booklet, Electronic Banking Booklet
- No. 193                    ‘Phishing’ and E-mail scams
- No. 196                    Information Technology Examination Handbook – Retail Payment Systems Booklet
- No. 199                    Information Technology Examination Handbook – Development and Acquisition Booklet
- No. 201                    Information Technology Examination Handbook – Management Booklet and Outsourcing Technology Services Booklet
- No. 204                    Information Technology Examination Handbook – Operations Booklet and Wholesale Payment Systems Booklet
- No. 205                    ‘Phishing’ Customer Brochure
- No. 207                    Interagency Guidance – Risk Management of Free and Open Source Software
- No. 214                    Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- No. 228                    Interagency Guidance on Authentication in an Internet Banking Environment
- No. 231                    Compliance Guide for Interagency Guidelines Establishing Information Security Standards

No. 237                      Interagency Advisory on Influenza Pandemic Preparedness

*Thrift Bulletins*

TB 81                        Interagency Policy Statement on the Internal Audit Function and Its Outsourcing

TB 82a                      Third Party Arrangements

TB 83                        Interagency Guidance on Weblinking: Identifying Risks and Risk Techniques

*Handbook Sections*

[Section 340](#)                [Internal Controls](#)

[Section 1300](#)              [Fair Credit Reporting Act](#)

[Section 1370](#)              [Electronic Banking](#)

[Section 1375](#)              [Privacy](#)



# Information Technology Risks and Controls Program

---

## EXAMINATION OBJECTIVES

To determine whether management effectively identifies and mitigates the association's information technology (IT) risks.

To determine whether the board of directors adopted adequate policies, procedures, and operating strategies appropriate for the size and complexity of the association's IT environment.

To determine that the association has a written information security program to comply with the requirements of the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), which implement Sections 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act) and 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

To initiate corrective action when policies, procedures, or controls are deficient or when you note violations of laws or regulations.

## EXAMINATION PROCEDURES

WKP. REF.

### LEVEL I

Level I procedures assess the association's processes for identifying and managing IT risks. Level I procedures are sufficient when an association has an effective internal control environment for IT risks, and there are no findings, which would cause you to expand your scope.

1. Review the association's response to the PERK 005, previous examination reports, including IT Reports of Examination, internal and external audit reports, and supervisory correspondence. After verifying completeness and accuracy of the IT database information, provide this information to your regional office for processing and input.

- 
2. Determine that the association implemented effective corrective actions for all previously cited IT exceptions, criticisms, or violations. This includes any matters cited in IT Reports of Examination.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

3. Determine the complexity of the association's information technology environment. Identify the association's significant systems. Significant means those critical to ensure information security, satisfactory customer service, and continuity of operations. Review the association's networks. Determine what significant applications are processed on the networks.

---
4. In conjunction with the Examiner-in-Charge (EIC) or examiner(s) performing the other Management programs, review board of directors' minutes of regular, special, and committee meetings for discussion and approval of significant IT matters. Examples of significant IT matters would include the association's written information security program, new or ongoing service provider relationships, and the association's business continuity plan.

---
5. In conjunction with the examiner(s) performing the reviews of Management and Earnings, determine the effectiveness of the board of directors and senior management in implementing strategic planning for IT. Evaluate plans for any significant changes. Review the association's strategic or business plan for IT-related activities.

---
6. Review the association's policies and procedures for IT. Determine whether these are effective for monitoring and controlling the association's IT risks considering the complexity of its IT environment.

---
7. In conjunction with the examiner(s) performing the review of the audit function, assess the adequacy of the association's audit coverage for IT risks. Verify that audit policies, practices, and programs for IT audits or other independent reviews are adequate for the size and complexity of the association's IT environment.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

8. Review IT audits or other independent reviews completed since the preceding examination. Determine that IT audit work products are adequate for the size and complexity of the association's IT environment.
- 
9. Assess management's responsiveness to IT audit concerns. Review the timeliness and adequacy of corrective actions. Confirm that the board of directors is informed of significant audit concerns, and that the board ensures completion of corrective actions.
- 
10. Determine that IT audit expertise and training are sufficient for the complexity of the IT risks of the association.
- 
11. Determine the association's compliance with the objectives of the interagency Security Guidelines implementing Sections 501(b) of the GLB Act and 216 of the FACT Act. The Security Guidelines require associations to have a comprehensive, written information security program that includes the administrative, technical, and physical safeguards to achieve the following objectives:
- Ensure the security and confidentiality of customer information.
  - Protect against any anticipated threats or hazards to the security or integrity of customer information.
  - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
  - Ensure proper disposal of customer and consumer information.

To meet the objectives and comply with the Security Guidelines, an association must:

- Implement a written information security program that the board of directors approved.

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

- Conduct and prepare a written information security risk assessment.
  - Require in contracts that service providers implement appropriate information security programs designed to meet the objectives of the Security Guidelines.
  - Monitor, evaluate, and adjust the information security program for changes in the association's IT environment.
  - Report to the board of directors annually regarding the association's compliance with the Security Guidelines and the status of the written information security program.
- 
12. Review measures the association has implemented in its written information security program to manage and control risks. Determine that the association considered and adopted, as appropriate:
- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals.
  - Controls and procedures to prevent employees from providing customer information to unauthorized individuals through pretext calling or other fraudulent methods.
  - Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.
  - Encryption of electronic customer information, including while in transit or in storage, or on networks or systems, to ensure unauthorized individuals do not gain access.
  - Procedures designed to ensure that modifications to customer information systems are consistent with the association's written information security program.
  - Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of misuse of customer information.
  - Monitoring systems and procedures to detect actual and attempted attacks or other intrusions into customer information systems.

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

- Response programs that specify actions to take when the association suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies .
  - Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.
- 

13. Confirm that the association has ongoing training for employees that implement and maintain the information security program. Review guidance to association employees for protecting customer and corporate information. Such guidance should describe the employee's responsibilities and consequences of improper actions.

---

14. Determine that the association has an incident response program consistent with the guidance in CEO Memo 214. Evaluate the effectiveness of the association's program for responding to incidents of unauthorized access to sensitive customer information and providing notification, as required. Confirm that the association's response program contains measures to:

- Assess the nature and scope of the incident.
  - Notify OTS, either directly or through the association's service providers.
  - Notify law enforcement agencies.
  - File Suspicious Activity Reports when required.
  - Control the incidents of unauthorized access.
  - Notify customers, when necessary.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

15. If the association had incidents of unauthorized access to sensitive customer information, determine that it:
- Conducted a prompt investigation to determine the likelihood the information accessed has been or will be misused.
  - Notified customers when the investigation determined misuse of sensitive customer information has occurred or is reasonably probable.
  - Delivered notification to customers, when warranted, by means the customer can reasonably be expected to receive, for example, by telephone, mail, or electronic mail.
- 
16. Review the association's customer notice and determine it contains:
- A description of the incident, including type of information subject to unauthorized access.
  - Measures taken by the association to protect customers from further unauthorized access.
  - Telephone numbers customers can call for information and assistance.
  - Reminders to customers to review account statements over a reasonable period – 12-to-24 months – and to report immediately suspicious activity and suspected identity theft incidents.
  - A description of a fraud alert and how to place one in a customer's report.
  - Recommendations to obtain credit reports from each nationwide credit-reporting agency and have information related to fraudulent transactions deleted.
  - An explanation of how customers can obtain free credit reports.
  - Information concerning availability of online guidance by the Federal Trade Commission regarding steps the consumer can take to protect against identity theft.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

17. Evaluate the effectiveness of the association's measures to authenticate customers accessing Internet-based services and other electronic banking activities. Ensure that the association's authentication methods and controls specifically address the need for risk-based assessments, customer awareness, and security measures consistent with the guidance in CEO Memo 228. An association should:

- Ensure its information security program identifies and assesses risks associated with Internet-based products and services, identifies risk mitigation actions, and evaluates customer awareness efforts.
  - Adjust its information security program for changes in IT, sensitivity of customer information, and internal or external threats to information.
  - Implement appropriate risk mitigation strategies.
- 

18. Review password controls used on the association's operating systems and significant applications. Confirm these address password length, change intervals, composition, history, and reuse or lockout. Assess the effectiveness of these controls.

---

19. Assess the association's user access assignment policies and procedures for its information systems. Determine that these policies and procedures:

- Provide for proper segregation of duties and dual controls.
  - Assign processing capabilities according to job responsibilities.
  - Limit system administrator capabilities appropriately.
  - Create user access profiles or user access assignments that are differentiated according to job duties.
  - Ensure that the association periodically reviews and updates user access assignments for job changes and terminations.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

20. Review user access profiles or user access assignments for at least one of the association's significant systems, for example, lending, deposits, general ledger, or funds transfers. Determine that system access rights are consistent with the association's policies and procedures for assigning system access.
- 
21. Confirm that the association has current written procedures to ensure security over its funds transfer activities, and that personnel are adequately trained to follow these procedures.
- 
22. Confirm that each authorized user involved in the association's funds transfer activities maintains a unique password known only to the user. Verify that system users change passwords frequently.
- 
23. Review the association's business continuity plan. Verify that the business continuity plan is based on a business impact analysis and that it identifies recovery priorities. Confirm that the association tested the business continuity plan within the past twelve months and that the board of directors annually approves testing results and the business continuity plan.
- 
24. Review the association's back-up procedures. Determine what data are backed up, the rotation schedule, where the back-up media are stored, and how soon the back-up media are taken offsite.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



# Information Technology Risks and Controls Program

---

WKP. REF.

25. Ensure that the association exercises appropriate due diligence in selecting, managing, and monitoring its service providers. Determine the association has established adequate policies and procedures to manage its service provider or vendor relationships.
- 
26. Determine that the association's contracts with its service providers have clauses that require the vendors to implement measures designed to meet the objectives of the Security Guidelines. Review the association's policies, procedures, and practices used to confirm that its service providers satisfied obligations under the contract regarding customer information.
- 
27. Determine that the association's board of directors, or an appropriate committee, approves new service provider relationships, or significant changes to existing outsourcing arrangements. These changes should be supported by a written risk analysis consistent with the association's business plan and the proposed or planned activity.
- 
28. Determine that association management and the board of directors periodically review significant service provider contracts and service level agreements.
- 
29. If the association created a transactional website since the previous exam determine that it provided the notice to OTS as required by CEO Memo 109. If the Notice was not timely and satisfactorily filed, contact the regional office to discuss appropriate remediation actions. Discuss with the regional office the need for follow-up review to ensure compliance with the requirements set forth in the CEO memo.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Information Technology Risks and Controls Program

---

WKP. REF.

30. Review the association's website to determine there are no inappropriate or misleading website links.

---

31. Discuss with your EIC any planned or pending system conversion, transactional website plans not previously communicated to or filed with OTS, system-generated errors that affect integrity of management information or regulatory reports, or any other significant IT issues or concerns. After discussion with your EIC, notify your regional IT Examination Manager, as appropriate.

---

## LEVEL II

After you complete the Level I examination procedures, if you need additional review to support an examination conclusion for a particular IT risk, you should review examination guidance and procedures in the FFIEC Information Technology Examination Handbook for the specific subject matter. These FFIEC Information Technology Examination Handbook procedures are considered Level II procedures for [Examination Handbook Section 341](#).

You should complete the examination procedures in the FFIEC Information Technology Examination Handbook you deem necessary to test, support, and present conclusions derived from performing Level I procedures. Level II procedures provide additional verification regarding the level of technology risk and the effectiveness of a savings association's risk management processes and controls. You can use the FFIEC examination procedures in their entirety or selectively, depending on the examination scope and need for additional verification.

## EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## External Audit

Accurate financial reporting is essential to an institution's safety and soundness. The board of directors and the audit committee are responsible for ensuring that their institution operates in a safe and sound manner. To achieve this goal and meet the safety and soundness guidelines implementing Section 39 of the Federal Deposit Insurance Act (FDI Act) (12 USCS 1831p-1) (see 12 CFR 510), the board of directors should ensure that their institution maintains effective internal controls (see Handbook Sections 340, [Internal Control](#), and 355, [Internal Audit](#)).

LINKS	
<a href="#">Program</a>	Management is responsible for effectively managing the institution's risks and making sound business decisions. They should also ensure that the financial statements fairly report the savings association's financial condition, results of operations, and cash flows, and that the institution prepares its financial statements in accordance with generally accepted accounting principles (GAAP).
<a href="#">Appendix A</a>	
<a href="#">Appendix B</a>	
<a href="#">Appendix C</a>	Savings institutions must provide accurate and timely Thrift Financial Reports by law (12 USC 1464(v)). These reports serve an important role in risk-focused supervision programs, by contributing to pre-examination planning, off-site monitoring programs, and assessments of an institution's capital adequacy and financial strength.
<a href="#">Appendix D</a>	
<a href="#">Appendix E</a>	

The OTS encourages all institutions to have an external audit. Some institutions must have an audit of the institution's financial statements by an independent public accountant (external auditor), or the OTS may require an audit of an institution's financial statements by an external auditor under certain circumstances. All audits of savings associations, regardless of size, must comply with the requirements outlined for management, the board of directors, and the external auditor in the FDICIA-required audit section below.

For institutions that do not have an external audit, other acceptable external auditing programs include:

- A balance sheet audit in accordance with generally accepted auditing standards (GAAS) by an external auditor.
- Attestation procedures that result in an external auditor's report on an institution's internal control over financial reporting (attestation report).
- Agreed-upon procedures or state-required examinations.

## FDICIA-REQUIRED AUDIT

## Audit of Savings Associations with \$500 Million or More of Total Assets

Section 112 of the Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991 and the Federal Deposit Insurance Corporation's (FDIC) implementing Regulation 12 CFR Part 363 requires savings associations with assets of \$500 million or more to obtain an audit of the financial statements by an independent public accountant.

Savings associations must comply with the provisions of the FDIC Regulation 12 CFR § 363.2, Annual Reporting Requirements. Savings associations should file the required reports with the FDIC and OTS (appropriate Regional OTS Office) in accordance with the provisions of this regulation.

[Appendix B](#) of this Section summarizes these provisions, and OTS audit requirements. Specific FDIC provisions in Appendix A of Part 363 are discussed below.

## Management:

- Prepare a statement declaring its responsibility for the annual financial statements.
- Establish and maintain an adequate internal control and procedures for financial reporting.
- As of the end of the fiscal year, assess the effectiveness of the internal control and procedures for financial reporting.
- Assess the effectiveness of the internal control and procedures for compliance with federal laws and regulations relating to loans to insiders and dividend restrictions.

## Board of Directors:

- Establish an audit committee consisting of outside directors who are independent of management. In no circumstances may an audit committee consist of less than a majority of outside directors. Exceptions to the independent membership requirement should be rare.
- Determine the duties of the audit committee that should, at a minimum, include reviewing the audit reports with the external auditor.

## External Auditor:

- Attest to whether management's assertion about the effectiveness of the internal control over financial reporting is fairly stated.
- Participate in a peer review program that is acceptable to the FDIC.

In addition, the FDIC requires the following reports:

- A management report on internal controls (management internal control report).
- An external auditor's attestation report on management's assessment of the effectiveness of internal control over financial reporting in Accordance with Statements on Standards For Attestation Engagements (SSAE) No. 10, Attestation Standards: Revisions and Recodification (AT 101).

### Information That Must Be Available to External Auditors

Section 931 of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA), (12 USC § 1817(a)), requires FDIC-insured associations that engage the services of an external auditor to audit the association within the past two years to provide copies of the following reports:

- The most recent report of condition, that is, the OTS Thrift Financial Report.
- The association's most recent Report of Examination (ROE).

In addition, savings associations must provide the external auditor with the following information:

- A copy of any supervisory agreement or memorandum of understanding or written agreement between a federal or state banking agency and the association that is in effect during the period covered by the audit.
- A report of any formal action taken by a federal or state banking agency during such period, or any civil money penalty assessed with respect to the association or any association-affiliated party.

Regulatory personnel should determine if the association is in compliance with § 931 of FIRREA and report instances of noncompliance to the Regional Accountant.

### Changes in Auditors

The FDIC requires the board of directors to provide a notice of termination or engagement of the external auditor (see 12 CFR §§ 363.2 and 363.4). In addition, the external auditor must provide the notice of termination (see 12 CFR § 363.3(c)) to the FDIC. OTS may request that the institution send notice to the appropriate supervisory office.

### *Work Paper Reviews*

The FDIC's policy is to review the audit work papers of Part 363 institutions that have been assigned, or expect to be assigned, a composite CAMELS rating of 4 or 5. The FDIC will coordinate the review with the institution's supervisory agency. For additional information on work paper reviews, see the discussion under Regulatory Concerns in this Handbook Section.

*Peer Review Reports*

FDICIA requires that firms performing audits on institutions with assets in excess of \$500M enroll in a peer review program, and that each firm files a copy of its peer review report with the FDIC. In a peer review program, one accounting firm basically examines another firm's quality control for accounting and auditing practices on selected engagements and functional areas. This review encompasses the organizational structure of the policies adopted and the procedures established by a firm to provide it with reasonable assurance that it complies with professional standards.

The Chief Accountant's office obtains copies of the peer review reports from the FDIC, and maintains an updated database that it periodically distributes to the Regional Accountants. OTS will make copies of the reports available upon request. If any firm has significant deficiencies noted in its peer review report, OTS staff will notify the Regional Accountant for further action.

**OTS-REQUIRED AUDIT****Audit of Savings Association Holding Companies with \$500 Million or More of Total Assets**

Under 12 CFR § 562.4, OTS requires a savings association holding company to obtain an audit of the financial statements by an external auditor when the total assets of the consolidated savings association subsidiary(ies) are \$500 million or more. The holding company should comply with the reporting requirements at Item 21, Financial Statements in the H-(b)11 Annual Report.

*Modification or Waiver*

OTS may grant a savings association holding company's request for a modification or waiver of the external audit requirement under any of the following circumstances:

- The savings association holding company engages in very limited activities other than control of subsidiary savings association(s) and it submits the subsidiary savings association's separate external audited financial statements.
- The accounting basis of the holding company makes consolidated financial statements or an external audit impractical.
- The external audit would represent an unusual and unreasonable regulatory burden.

The savings association holding company must make a written request for a waiver to OTS's Regional Director or designee. The request must describe the circumstances that the savings association holding company believes warrant the proposed modification or waiver.

## Audit of Savings Associations That Receive a Composite CAMELS Rating of 3, 4, or 5

OTS requires savings associations, without regard to size, that receive a composite CAMELS rating of 3, 4, or 5, as of its most recent safety and soundness examination, to obtain an audit of its financial statements by an external auditor.

### *Required Reports*

In addition to the audited financial statements, the savings association must submit:

- Any audit-related reports including, but not limited to, internal control reports from the external auditor that contain conclusions and recommendations related to the audit.
- Any other OTS-requested supplemental information, or schedules.

OTS accepts the audited consolidated financial statements of the savings association holding company in lieu of separate audited financial statements of the savings association.

### *Filing Requirements*

If OTS requires a savings association to obtain an audit, it must forward three copies of the required reports to the Regional Director or designee within 90 days of the fiscal year-end, or within 15 days of receipt, whichever is earlier.

When a savings association with a composite CAMELS rating of 3, 4, or 5 has assets of \$500 million or more, it must file either the required savings association audit report, or the consolidated savings association holding company audit report, with both the FDIC and OTS. The filings should comply with FDIC Regulation Part 363 and FDIC guidelines at Appendix A to Part 363.

### *Waivers*

A savings association may dispense with an audit if OTS determines that an audit is not the most effective means to address the safety and soundness concerns that caused the composite CAMELS rating of 3, 4, or 5. The waiver provision only applies to OTS required audits. It does not apply to audits required by public securities filing requirements, or § 112 of FDICIA and the FDIC implementing Regulation 12 CFR Part 363. The savings association must make a written request for a waiver to the OTS Regional Director or designee. The written request must include:

- The basis for the composite CAMELS rating of 3, 4, or 5, and the specific reasons why the savings association believes an audit would not address the source of the safety and soundness concerns in the most effective manner; and
- As an alternative, specify procedures and describe how they will address the source of the safety and soundness concerns identified by the examination; or

- Indicate the reasons why they consider an alternative to an audit as unnecessary.

OTS will respond to a timely request for an audit waiver from the savings association.

## Safety and Soundness Considerations for Granting Waiver Requests

OTS may grant a savings association's request for a waiver of the external audit requirement if the CAMELS rating of 3, 4, or 5 is due to safety and soundness concerns that an external audit would not effectively address.

Safety and soundness concerns may include areas of supervisory judgment. Often the association cannot reduce these areas to objective criteria that can be audited effectively. Safety and soundness concerns may represent areas in which you have specialized knowledge and expertise; or the concerns may represent areas normally not included in the scope of an external audit.

Under such circumstances, you may consider requesting specific procedures to address these areas. You may also rely on your judgment about other procedures that will specifically address your supervisory concerns. Examples of these areas include the following circumstances:

- Adequacy of capital levels.
- Deficient credit underwriting policies and loan documentation that management is correcting.
- Low level of earnings or poor quality of earnings whose source the examiners investigated in a recent examination and management is correcting.
- Liquidity, interest rate risk, and other safety and soundness or compliance matters.

While recognizing the limits of an external audit, there are circumstances when pervasive safety and soundness concerns warrant an external audit. These include, but are not limited to the following concerns:

- Identified weakness in the internal audit function or the internal control structure and procedures for financial reporting.
- Lack of confidence in the board of directors or management with regard to integrity, ethical values, competence, operating philosophy, and overall corporate governance exercised by the board.
- Questionable transactions with affiliates.



### Case-by-Case Safety and Soundness Required Audit

OTS may require at any time, for any safety and soundness reasons identified by the Director, an independent audit of the financial statements of, or the application of procedures agreed-upon by OTS to, a savings association, savings association holding company, or affiliate by an external auditor.

### Audit of De Novo Savings Associations

OTS generally requires an external audit as a condition of approval for de novo savings associations. The conditions of approval will describe the reporting and filing requirements.

### Notification by OTS of Audit Requirement

When OTS requires an entity to obtain an external audit for reasons other than its CAMELS rating or size, OTS's Regional Director will notify, in writing, the savings association or savings association holding company.

### Audit of Trust Activities

Audit requirements for institutions with permission to exercise fiduciary powers are in 12 CFR §§ 550.440 through 550.480. Those institutions should also refer to the Trust and Asset Management Regulatory Handbook for audit requirements, policies, and procedures.

## OTS-REQUIRED AGREED-UPON PROCEDURES

OTS may require a savings association, savings association holding company, or affiliates to obtain the services of an external auditor to perform agreed-upon procedures to address certain aspects of an entity's operations, operations at outside servicers, adherence to specified laws, regulations, policies and accounting principles, or other specific concerns.

OTS may require an entity to obtain specified procedures, under any of the following conditions:

- When the examination process will not address supervisory concerns for the specified element, account, items of the financial statements, outside servicer, or other matters.
- When the specified procedures could supplement the examination process.
- When an external audit is not the most effective means to address the specified element, account, items of the financial statements or other matters of supervisory concern.
- When identified or suspected insider abuses exist.
- When there is identified or suspected defalcation.
- When there is identified or suspected criminal activity.

- When objective criteria exist for reasonably measuring compliance with specified laws, regulations, and policies.

### Notification by the OTS

OTS's Regional Director, or designee, will notify the entity in writing, when we require it to engage the services of a qualified external auditor to perform agreed-upon procedures.

### Required Procedures and Reports

Once you determine that agreed-upon procedures are an effective means to address the safety and soundness concerns, identify the specific elements, accounts, items of the financial statements, or other matters that the external auditor and the institution must address.

OTS generally requires the external auditor to perform the procedures. The external auditor must report in accordance with GAAS for attestation engagements. OTS may also provide such procedures directly, or develop procedures in consultation with the external auditor.

### Filing Requirements

If OTS requires an entity to obtain agreed-upon procedures, the institution must forward three copies of the specified procedures report to the Regional Director, or designee, within 30 days of receipt of the report, or 30 days from the date of the procedures, whichever is less. The entity must also forward a copy of the signed engagement letter to the Regional Director, or designee, before the external auditor conducts fieldwork.

### Auditor Requirements For Required Audit or Required Agreed-Upon Procedures

The external auditor or other qualified person who performs the audit or the agreed-upon procedures must meet the following minimum requirements at OTS Regulation § 562.4(d)(1), (2), (3), and (4):

- Be registered or licensed to practice as a public accountant, and maintain good standing, under the laws of the state or other political subdivision of the United States where the home office of the entity is located.
- Agree in the engagement letter to provide copies to OTS of any work papers, policies, and procedures relating to services performed pursuant to § 562.4. [See Appendix D for a sample letter to request audit work papers.](#)
- Comply with the American Institute of Certified Public Accountants (AICPA) Code of Professional Conduct, and meet the Securities and Exchange Commission's (SEC) independence requirements.

- Receive, or be enrolled in, a peer review. The OTS accepts the following peer review guidelines:
  - The external peer review should be generally consistent with AICPA standards.
  - An organization independent of the auditor or firm being reviewed should conduct the review.
  - The organization should conduct a review at least as frequently as is consistent with AICPA standards.
  - The external peer review should include, if available, at least one audit of an insured depository institution or consolidated depository institution holding company. (The external auditor should make the peer review report available to the OTS upon request).
  - The auditor or firm under review should take corrective action required under any qualified peer review report on a timely basis.

## AUDITS REQUIRED BY SEC AND OTS FOR PUBLIC SECURITIES FILING PURPOSES

Holding companies of savings associations and subsidiaries of savings associations (service corporations and operating subsidiaries) that offer public securities must register and file appropriate documents with the SEC. If a savings association, rather than a holding company or subsidiaries, lists securities on a stock exchange and has more than 500 stockholders, it must register the securities, and file its reporting documents, with OTS under Section 12 of the Securities Exchange Act of 1934 ('34 Act). Section 12(i) of the '34 Act assigns the reporting functions to OTS for thrift securities and grants OTS the power to make rules and regulations to execute these functions. Section 3(a)(5) (15 USC § 77c(a)(5)) of the Securities Act of 1933 ('33 Act) exempts thrift securities from registration with the SEC under the '33 Act. The rules and regulations for public offerings of a savings association are in 12 CFR Part 563g.

Regulations under 12 CFR Part 563c establish the qualifications and independence requirements for an external auditor engaged to perform services for companies with a class of securities registered pursuant to the Securities Exchange Act of 1934. The qualifications and independence requirements in 12 CFR Part 563c are generally consistent to those issued by the SEC.

To perform these services, the external auditor should be registered and in good standing under the laws of the place of his or her residence or principal office. Neither the external auditor nor the associated auditing firm should have acquired, or have a commitment to acquire, any direct financial interest or any material indirect financial interest in the company. In addition, neither should be connected to the company as a promoter, underwriter, voting trustee, officer, or employee. At least annually, the external auditor should disclose to the audit committee in writing the relationship between the auditor and its related entities that, in the auditor's professional judgment, may reasonably bear on

independence. The external auditor should further state that he or she is independent of the company, as well as discuss independence with the audit committee.

If the institution produces interim financial reports, the external auditor must review the financial statements prior to inclusion in the quarterly 10-Q reports using procedures in Statement on Auditing Standards (SAS) No. 71, *Interim Financial Information*. SAS No. 71, as amended by SAS No. 90, requires the external auditor to discuss the quality of the institution's accounting principles with the audit committee before filing the information. The auditor can limit the quarterly discussion to the impact of significant events, transactions, and changes in accounting estimates the auditor considered in performing the review procedures.

The audit committee has several responsibilities with regard to the external audit for public filing savings associations. For listed companies with a market capitalization above \$200 million, the audit committee, as part of proxy and information statements for meetings at which directors are elected, must report whether the audit committee performed the following functions:

- Reviewed and discussed audited financial statements with management.
- Communicated with the company's external auditor any matters required to be discussed under SAS No. 61, *Communications with Audit Committees*. SAS No. 61, as amended by SAS Nos. 89 and 90, requires the external auditor to discuss the "quality, not just the acceptability" of a company's accounting principles with the audit committee. The discussion must be "open and frank, and generally should include such matters as the consistency of the entity's accounting policies and their application, and the clarity and completeness of the entity's financial statements, which include related disclosures."
- Received the written disclosures and the letter from the external auditor, and discussed the external auditor's independence with the external auditor.
- Recommended to the board of directors that the company's annual report or Form 10K include the audited financial statements.

Savings associations must include certain information about their audit committee in a proxy statement (Schedule A, Item 7). If the registered savings association has an audit committee, the proxy statement should provide the following items:

- Audit committee information required under SEC regulation 17 CFR Part 229.306 (Regulation S-K, Audit Committee Report).
- Board of director adoption of a written charter for the audit committee. The charter should specify the following:
  - The scope of the audit committee's responsibilities, and how it carries out its responsibilities.

- That the external auditor is ultimately accountable to the board of directors and the audit committee.
- That the board of directors and audit committee has the authority and responsibility to select, evaluate, and replace the external auditor.
- A copy of the written charter, if any, as an appendix to the proxy statement at least once every three years.

If there is no audit committee, the names of the board committee performing the equivalent functions or the names of the entire board must appear.

The NYSE, AMEX, and NASD require listed companies to disclose whether audit committee members are independent. Under their rules, if a member is not independent, then the institution should disclose the nature of the relationship that makes the member not independent, and list the reasons for the board's determination. Even if not listed on one of the above exchanges, the institution should disclose whether audit committee members are independent. In 2000, the above exchanges expanded their definition of independence for audit committee members. In general, membership is precluded from the audit committee if any of the following apply to the individual:

- Is currently employed with the company or an affiliate.
- Is currently employed, or has held employment in the past three years, with the current parent of predecessor company.
- Is currently, or within the past three years, has been a member of the immediate family of a current executive officer of the company or an affiliate.
- Is currently an executive of another business organization where any of the company's executives serve on the organization's compensation committee.
- Is currently a partner, controlling shareholder, or executive officer of a business organization that has a business relationship with the company.
- Currently has a direct business relationship with the company.

These rules also require that at least three audit committee members, each of whom must be, or become, "financially literate," include one member with accounting or financial expertise. To be financially literate, the member should be able to read and understand financial statements, including a balance sheet, income statement, and cash flow statement.

## VOLUNTARY EXTERNAL AUDITING PROGRAMS

### Audit of Savings Associations with Less Than \$500 Million of Total Assets

#### *Audit Committees*

To ensure the adequacy of its internal and external auditing programs, OTS encourages the board of directors of each institution that is not otherwise required to do so to establish an audit committee consisting entirely of outside directors. If this is impracticable, the board should organize the audit committee so that outside directors constitute a majority of the membership.

The audit committee's duties may include reviewing the independence of the external auditor annually, reviewing and approving the annual audit plans and external audit engagement, consulting with management, overseeing performance and setting expectations for the roles of both internal and external audits, seeking an opinion on an accounting issue, and overseeing the quarterly regulatory reporting process.

The audit committee may become involved in emerging issues, key business decisions, ventures, and associated risks. It may also maintain dialog with regulators. The audit committee should report periodically to the full board of directors.

At least annually, the board or audit committee should review the institution's activities that present significant financial reporting risks. The board or audit committee should consider the potential benefits of an audit of the institution's financial statements or the institution's internal control over financial reporting, or both. They should also consider additional procedures for a particular year or several years to cover areas of particularly high risk or special concern. The board should record their reasons supporting their decisions in the minutes.

Based on its review, the board should select an external auditing program that is appropriate for the institution considering its risks, size, and the nature, scope, and complexity of its activities. As an important component of an institution's overall risk management process, an external auditing program, as discussed in this Section, represents procedures performed, generally by an external auditor, to test and evaluate high-risk areas of an institution's business. The procedures should be sufficient for the external auditor to express an opinion on the financial statements or to report on the results of the procedures performed.

#### *Types of External Auditing Programs for Voluntary Audits*

OTS encourages all OTS-regulated institutions to have a full-scope financial statement audit. In lieu of a full-scope financial statement audit, institutions not required to have an audit may elect a balance sheet audit or an attestation report on internal control assertions as the external auditing program. The external auditor performs these types of external auditing programs. Agreed-upon procedures or state-required examinations are also acceptable.

### *Financial Statement Audit*

In a financial statement audit, the external auditor expresses an opinion on the fairness with which the financial statements present, in all material respects, the financial position, results of operations, and cash flows, in conformity with GAAP. The auditor will also state if the audit was in accordance with GAAS. The auditor identifies those circumstances in which the institution did not consistently observe GAAP in the preparation of the financial statements for the current period, and should obtain reasonable assurance that material misstatements are detected.

### *Balance Sheet Audit*

As an alternative, the external auditor may perform a balance sheet audit. A balance sheet audit is an audit of an institution's balance sheet and any accompanying footnotes. The external auditor performs the balance sheet audit in accordance with GAAS. It should be of sufficient scope to enable the auditor to express an opinion on the fairness of the balance sheet presentation in accordance with GAAP.

### *Attestation Engagement*

Another alternative is an attestation engagement. In an attestation engagement, management evaluates and documents its review of the effectiveness of the institution's internal control over financial reporting in the identified risk areas as of a specific report date. Management should prepare a written assertion that specifies the criteria management used to evaluate the effectiveness of the institution's internal control for financial reporting in the identified risk areas. The written assertion should state management's opinion on the effectiveness of internal control for this specified financial reporting. Under SSAE No. 10, if management refuses to provide the external auditor with a written assertion, the auditor should include a reference to a scope limitation, and accordingly, modify his or her engagement report.

In an attestation engagement, the external auditor performs tests on the internal controls of the specified financial reporting in order to attest to management's assertion. If the external auditor concurs with management's assertion, even if the assertion discloses one or more instances of material internal control weakness, the auditor provides a report attesting to management's assertions.

### *Agreed-Upon Procedures*

Agreed-upon procedures are procedures specified by the institution and the external auditor or other qualified person to test activities in certain areas. For state-required examinations, states may specify the procedures and require institutions to have these procedures performed annually by their directors or other independent persons.

Agreed-upon procedures do not involve reporting on the fairness of the institution's financial statements or attesting to the effectiveness of internal control over financial reporting. The external auditor or other qualified person presents the procedures and the findings or results of the procedures to the board or the audit committee so that they may draw their own conclusions regarding work performed.

The board of directors should consider whether an external auditor or other qualified person should perform the agreed-upon procedures or the procedures required for the state examination. If performed by an external auditor, the auditor must conduct the work under, and may be held accountable for departures from, professional standards. However, agreed-upon procedures engagements require different professional standards than those used for an audit of an institution's financial statements or its balance sheet.

OTS expects institutions that historically have had an audit of their financial statements by an external auditor or other type of external auditing program to continue to do so. For those that have another type of external auditing program, OTS expects them to continue to have the same, or a more extensive, external auditing program in the future.

### Requested Reports For Voluntary External Auditing Programs

***OTS requests that all savings associations and savings association holding companies that voluntarily obtain an audit of the financial statements, or have some other type of external auditing program performed, file any and all audit-related reports with the appropriate regional office.***

OTS also requests that all institutions notify the appropriate supervisory office when they initially engage an external auditor, or when they change or terminate the services of their auditor. See [Appendix C, Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations](#).

The preferable time for an institution to schedule the performance of an external auditing program is as of an institution's fiscal year-end. However, any quarter-end date that coincides with a regulatory report date provides similar benefits.

Generally, check whether the institution has filed its external auditing reports with its supervisory office. If not, you should request a copy of the most recent reports during the periodic safety and soundness examination.

### Auditor Selection

OTS requires that an external auditor who meets the minimum requirements described in 12 CFR § 562.4(d)(1), (2), and (3) for required audits conduct the voluntary audit of the financial statements. If an institution chooses a balance sheet audit or attestation engagement as its external auditing program, an external auditor who meets the minimum 12 CFR § 562.4(d)(1), (2), and (3) requirements should also perform these programs. Unlike required audits, the regulations do not require auditors performing voluntary audits to receive, or be enrolled, in a peer review.

Preferably, an external auditor will also perform agreed-upon procedures or procedures for a state-required examination. The external audit firm or other qualified persons selected to conduct an external auditing program and their staff carrying out the work should have experience with financial institution accounting and auditing, or similar expertise, and should be knowledgeable about relevant laws and regulations.



## Review of Voluntary External Auditing Programs

In your review of voluntary external auditing programs, you should consider the following factors:

- An institution's size.
- The nature, scope, and complexity of its business activities.
- Its risk profile.
- Actions taken to remedy identified weaknesses.
- The extent of its internal audit program.
- Compensating controls.

You should exercise judgment and discretion in evaluating the adequacy of an institution's external auditing program. Reports from voluntary external audits and external auditing programs should receive the same level and type of review as those submitted pursuant to FDICIA-required and OTS-required audits.

## AUDIT OF FINANCIAL STATEMENTS BY AN EXTERNAL AUDITOR (AUDIT)

### Objective of Financial Accounting

The fundamental objective of financial accounting is to provide reliable financial information about economic resources and obligations of a business enterprise.

### Objective of an Audit

Similar to the objective of financial accounting, the fundamental objective of an audit conducted in accordance with GAAS is to determine whether the financial statements fairly present, in all material respects, the financial position, results of operations, and cash flows of the institution in accordance with GAAP.

The audit should provide reasonable assurance that the financial statements are free of material misstatements, whether caused by error or fraud. Informative disclosures in the financial statements must follow GAAP, or the report must state otherwise.

### Audit Standards

External auditors should follow the AICPA Code of Professional Ethics. It requires that auditors perform external audits according to GAAS. GAAS, as distinct from accounting standards, are

concerned not only with the auditor's professional qualifications, but also the judgment the auditor exercises in the performance of an audit and with the quality of the audit procedures. There are three categories of GAAS:

- General standards.
- Fieldwork standards.
- Reporting standards.

The general standards require that the person, or persons, who performs the audit meet the following professional qualifications:

- Possess adequate technical training and proficiency.
- Maintain independence in mental attitude.
- Exercise due professional care in the performance of the audit and the preparation of the report.

Fieldwork standards include the following requirements:

- Adequately planned work.
- Properly supervised assistants, if any.
- Proper study and evaluation of existing internal controls to determine audit scope, audit procedures, and the extent of testing.
- Sufficient evidence to formulate an opinion on the financial statements under audit.

Reporting standards require that the external auditor state whether the institution presents its financial statements in accordance with GAAP.

### Limitations of Audits and Audited Financial Statements

Although auditing standards require the use of due care and professional skepticism, a properly designed and executed audit does not guarantee that the audit will detect all misstatements of amounts or omissions of disclosures in the financial statements. Moreover, an external audit is not designed or executed for regulatory purposes, and thus, does not guarantee that the auditor addressed OTS safety and soundness considerations. You should be cognizant of these and other limits inherent in an audit. The following examples illustrate some common limitations of audits:

- The auditor is not responsible for deciding whether an institution operates wisely. An unqualified audit report means that the association reports transactions and balances in

accordance with GAAP. It does not mean that the transactions make business sense, that the association manages associated risks in a safe and sound manner, or that the association can recover balances upon disposition or liquidation.

- The auditor attempts to understand financial reporting internal controls sufficient enough to plan the audit, and determine the nature, timing, and extent of tests to perform. This does not mean that the external auditor extensively reviews controls over all areas. The external auditor may use various levels of testing depending on the risk of a specific area.
- The auditor's report states that the financial statements present fairly the financial position. This means that, given evidence and current environment, the association can recover reported assets in the normal course of business. It does not mean that underwriting standards, operating strategy, loan monitoring systems, and workout procedures are adequate to mitigate losses if the environment changes.
- GAAP financial statements offer only limited disclosures of risks and uncertainties, and other safety and soundness factors on which an institution's viability depends.

## REGULATORY CONCERNS

The following documents are part of the supervisory process for monitoring savings associations:

- Audited financial statements along with the external auditor's report.
- External auditor's attestation report on internal control report over financial reporting, if applicable.
- External auditor's management letter.

When OTS or the FDIC requires an external audit, the audit must be completed on a timely basis. The regional office is responsible for determining that each association files a required audit report on a timely basis. The regional office should date stamp the required audit report upon receipt.

For required external audits, OTS policy requires savings associations to submit copies of the audit report, attestation report on internal control over financial reporting, and any other audit-related reports to the regional office. The regional office must maintain one complete set in the supervisory files (supervisory file copy) attached to the completed Audit-Related Report Checklist found in [Appendix A](#) of this Handbook Section. You should receive another set (examination file copy) with a copy of the appropriate checklists.

For all types of audits, required or otherwise, Regional staff should consider maintaining a tracking system of external audits by savings associations, which would include the name of the auditor, and various other information.

When OTS or FDIC requires an audit examination, examination managers are responsible for the review and timely follow-up of the various audit reports and correspondence. They should review audit reports, financial statements, reports on internal control and other audit-related reports within 90 days of receipt. Examination managers should add any items of supervisory interest to the supervisory concerns, objectives, and strategies section of the regulatory profile. Based on this review, the examination manager should take the following steps:

- Set out the timing and nature of any required follow-up as indicated on the checklist.
- Update the activity agenda section of the regulatory profile to reflect any planned actions resulting from the review.
- Consult the Regional Accountant when the follow-up includes issues about GAAP, GAAS, or enforcement matters.

OTS will generally reject, as unsatisfactory, a report of audit disclaiming an opinion on the audited financial statement, unless the reason for the disclaimer is beyond the control of the association or the Regional Accountant approves it.

The regional office is also responsible for requesting external auditing program reports from institutions not required by regulation or otherwise to have an external auditing program.

Chapter 18 of the AICPA Audit and Accounting Guide, Audits of Banks and Savings Institutions (May 1, 2000), and AICPA Statement of Auditing Standards No. 58 describe the standard types of audit reports. The Regional Accountant maintains copies of these materials.

## Audit Requirements

Reports from voluntary external audits and external auditing programs should receive the same level and type of review as those submitted pursuant to FDICIA-required and OTS-required audits.

## Independence of External Auditor

The audit committee should hire and terminate the external auditor. To maintain independence from management, the external auditor ideally reports to the outside directors of the board. You should question the independence and objectivity of the external auditor when the auditor appears to be reporting to management, appears to be an advocate for management, or generally appears to be working more for management than the board of directors.

Instances in which you should question independence include but are not limited to the following examples:

- Management approves the external auditor's presentations to the board

- Management prevents the external auditor from meeting with the board unless management was present
- The board of directors appears to lack the sophistication to understand or appropriately discuss audit or accounting issues with the external auditor
- The auditing staff does not have unrestricted access to the board or audit committee without management knowledge or approval.

Under these circumstances, you may decide to test the independence of the auditor through reviews of loan listings, contracts, stockholder listings, and other appropriate measures.

See also AICPA Interpretation (101-13) and rulings (101, 103, 104, and 105) regarding independence standards.

You should refer any concerns about independence to the Regional Accountant. The Regional Accountant may consult with the Chief Accountant.

## Review of External Audit Work Papers

### *Purpose and Benefits*

The purpose of reviewing external audit work papers is to gain insight into the scope of the external auditor's work and assessment of the financial condition of the institution. To assess the financial condition of the institution, the external auditor performs procedures that evaluate the reliability of financial statement assertions based on GAAS. A review of the external audit work papers and conversations with the external auditor should provide you insight into the following areas:

- The complexity of an institution's transactions.
- The extent of an institution's transactions that are assumption driven.
- The scope, extent, and depth of the external auditor's external audit work.
- The material weaknesses and reportable conditions regarding an institution's internal control and financial reporting practices.
- The accuracy and completeness of Thrift Financial Report (TFR) information.
- The reliability of the institution's assertions made in the TFR.

A review of the external audit work papers should assist you in the following activities:

- Performing financial analyses of the institution.

- Identifying areas of concern or accounting complexity. For example, the audit work papers may document management's reasons for an aggressive accounting practice. After the review, you should understand management's rationale, and assess whether a less aggressive accounting practice is more appropriate from a safety and soundness standpoint.
- Detecting trends and information not otherwise revealed in the monitoring process.
- Determining the scope of the examination:
  - You may reduce the scope of the examination in certain areas based on the extent, scope, and findings of the external audit work.
  - You may expand the examination scope in certain high-risk areas based on the external audit work.
  - You may expand the scope in certain areas based on the external auditor's findings that disclose matters of supervisory concern.
- Evaluating the institution's internal control over financial reporting. If an association has serious internal control weaknesses or deficiencies, you should discuss the full extent of such problems with the external auditor to determine whether you should expand the scope of the examination.
- Identifying areas where external audit work can supplement examination procedures.
- Identifying external audit work that provides insight into certain financial statement assertions, or that is sufficient to enable you to limit certain examination procedures. For example, the external audit work papers may document management's methodology for assessing the appropriate level of allowance for loan and lease losses or valuation estimates, including the assumptions and methodologies used to value servicing and residual assets. The external audit work papers should document the specific audit procedures performed to test and analyze those estimates. After the review, you should understand management's approach and any exposure areas. If the findings are acceptable for safety and soundness purposes, you may use the information to plan and supplement the examination procedures in this area.

Other benefits realized from external audit work paper reviews are:

- Discovering policy and procedures, or transactions and balances, subject to additional examination procedures.
- Developing an understanding of the external auditor's risk assessment process.
- Developing an understanding of management's support for certain transactions and balances.

- Improving examination focus. You may find that you can concentrate on high-risk areas and de-emphasize areas that have been adequately covered by the audit.

There are certain situations that may necessitate requesting the external audit work papers for review. Situations that might trigger an external audit work paper review include the following examples:

- The institution holds assets and liabilities subject to significant management judgment regarding valuation. Examples include the following assets and liabilities:
  - High-risk loans.
  - Repossessed assets.
  - Debt securities with significant credit loss concerns.
  - Servicing assets, if material.
  - Residual interests from securitizations, in which the carrying value is not readily determined by market quotes.
  - Significant potential losses from litigation.
  - Other off-balance sheet activities.
- New or outstanding securitization activities including private-label securitizations and other complex transactions.
- Material loan amounts serviced by others.
- Significant balances or changes in Other Assets or Other Liabilities.
- Significant business plan changes that affect organizational goals, including new or growing business lines.
- Recent acquisition or disposition transactions, including purchase business combinations.
- Institutions with significant goodwill and other intangible assets.
- Problematic computer processing that reinforces the need for general ledger account reconciliation.
- Large number of adjusting journal entries and/or significant balance sheet changes that would affect general ledger account reconciliation.
- Reported earnings or other financial measures substantially better than peer group.

- Institutions engaging in aggressive income recognition.
- Strained relationship between management and/or the board of directors and the external audit firm.
- Significant changes in the external audit program including recent unexplained or sudden change in external audit firm.
- Recent unexplained delays in issuance of audited financial statements.
- Issues regarding independence, objectivity, or competence of the external auditor.
- Accounting or internal audit staff that is inadequate in relation to the size, nature, complexity, and scope of activities of the institution.
- Recent or significant turnover in accounting or internal audit staff.
- Significant transactions with owners (parent company or stockholders), affiliates, Special Purpose Entities, or other related parties.
- Significant changes in Due To/Due From accounts.
- History of late TFR filings or TFR amendments.
- Significant safety and soundness concerns.
- Large unexplained reserves, suspense accounts, or large tax reserves.

If external audit work papers exist for lower-risk areas, such as confirming loans, and they appear accurate and reliable, you may use them to avoid duplicating efforts to gain the same or similar information. However, when you use external audit work papers in lieu of performing the actual work yourself, you are placing reliance on a work product not necessarily designed for regulatory purposes. In high-risk areas where the external audit work appears reliable, the work papers may be used to design and supplement examination procedures accordingly.

### Coordination with Regional Accountant

After reviewing work papers, refer any of the following concerns to the Regional Accountant:

- Regulatory reporting issues.
- The need for expanded verification procedures.
- Questions about the application of GAAP, GAAS or Statements on Standards for Attestation Engagements (SSAE).



- Unacceptable diversity in practices.<sup>1</sup>
- Deficiencies, in general.

The Regional Accountant will assist you in choosing a course of action, which may be to discuss the issue with the auditor in an attempt to resolve it. In addition, the Regional Accountant may consult with other appropriate divisions, such as the Chief Accountant, Enforcement, and/or Compliance.

### Obtaining External Audit Work Papers

OTS policy requires that the auditor agree in the engagement letter to provide access to and copies of any work papers, policies and procedures related to services performed. (12 CFR § 562.4(d)(2)).

If possible, the field manager or the assigned EIC should evaluate the need to review external audit work papers prior to the beginning of the exam. If the institution is known to have activities that trigger a review of external audit work papers, the field manager or EIC should make arrangements for the work papers to be available as soon as possible. This will facilitate using the results to tailor the scope of the examination review.

The request for access to the audit work papers should be in writing and addressed to the external auditor with coordination through the Regional Accountant. While the Regional Accountant need not participate in the audit work paper review, he or she will act as the liaison and participate if necessary. There are instances when the Regional Accountant does not necessarily need to get involved. These would include routine reviews where significant accounting issues are not expected. However, there are times when the Regional Accountant should be actively involved. For example, include the Regional Accountant when reviews involve the implementation of a significant new accounting pronouncement.

Auditors are generally cooperative, as they are interested in assessing the effect of examination concerns on the financial statements. The review of audit work papers and the discussion of significant items and complex transactions with the external auditors can help you assess whether the financial reporting is safe and sound.

The auditor may request that you “acknowledge” certain representations and conditions set forth in a letter from the auditing firm before allowing you access to or releasing to you copies of the work papers. It is not unreasonable for the auditor to request that you acknowledge receipt of documents. This is a common business practice and their proof of compliance with your request. OTS policy allows you to sign a document only to acknowledge receipt of an accounting firm’s letter and any copies of work papers,<sup>2</sup> policies, and procedures delivered with such letter. However, any attempt by an auditor to impose conditions, agreements, or understandings on you or OTS is contrary to the auditor’s

---

<sup>1</sup> Industry practice may have moved from the acceptable range of GAAP to outside of the range.

<sup>2</sup> When OTS requests copies of external audit work papers, the audit firm personnel generally make the photocopies for you. This allows the audit firm to maintain control over the work papers. When you have questions, call your Regional Accountant.

agreement in the engagement letter. Therefore, do not sign any document that implies that OTS has agreed to any conditions in the letter.

Notify the Regional Accountant if any external auditor seeks to avoid inclusion of the required agreement in the engagement letter under OTS Regulation 12 CFR 562.4(d)(2), or to evade, or impose conditions, on the obligation to provide OTS access to or copies of work papers, policies, and procedures relating to services performed. We provide a sample copy of a letter to request work papers in [Appendix D](#) and an acknowledgement letter in [Appendix E](#).

In limited circumstances, a subpoena may be necessary to gain access to the external audit work papers. In these cases, the examination staff and the Regional Accountant will contact Regional Enforcement and arrange for the subpoena. In these cases, you will provide written findings to the Regional Director.

#### *FDIC Policy for Audit Work Paper Review*

The FDIC issued guidance stating that it will review audit work papers for each insured institution subject to Part 363 that has been assigned, or expects to be assigned, a CAMELS rating of 4 or 5. In each case, the FDIC will contact the institution's primary federal regulator to arrange, if possible, a joint review of the work papers. When a savings association is an OTS-supervised institution, the FDIC indicates that it will contact the appropriate OTS supervisory office to determine in what manner, and which agency should notify the institution of the upcoming review. After the OTS supervisory office and the FDIC make that determination, one agency will inform the institution in advance that the agencies are contacting the auditor to request audit work papers. One agency will also notify the holding company.

#### Communications with Auditors

When conducting an audit of the financial statements of a savings association, the external auditor can consider, in accordance with GAAS, the regulatory authorities as a source of competent evidential matter. Accordingly, the external auditor may review communications from, and make inquiries of, the regulatory authorities. We encourage savings associations and their auditors to confer with OTS when they consider it appropriate. Such contacts may include meetings with you to assist in planning audits, or auditors may attend examination planning, interim, and exit conferences with association management and examiners. They may also attend other meetings between management or the board of directors (or a committee thereof) and examination personnel when you consider it appropriate.

You should provide associations with advance notice of the starting and completion dates of examinations so management can coordinate the audit fieldwork with the examination. Management should inform auditors in advance of scheduled examinations and meetings.

When requested by the association and the auditor, the examination manager may communicate examination findings prior to the completion of the examination. We encourage the examination manager to comply with such requests. This fosters better communications and improves the quality of financial reports. We also encourage you to communicate with auditors in the field after notifying the examination manager. You should communicate to the auditor all supervisory concerns and information except those involving confidential enforcement actions, such as imminent

conservatorships or receiverships. As a general guideline, you should communicate interim examination findings whenever the following occurs:

- The examination process results in substantiated findings that significantly affect the financial information reported by the association.
- The association is about to report quarterly or annual financial information to the OTS or other outside parties, such as shareholders or the general public.

Obviously, under such circumstances, prompt communication is important. Material examination adjustments made shortly after an association issues a financial statement can cause significant public disclosure and securities problems.

The regional office should make examination work papers available to external auditors upon request. If you have not issued the ROE, stamp any copies of work papers provided to the external auditor as "DRAFT." To access work papers, the external auditor must make the request in writing to the examination manager. The examination manager may decline requests for good cause but such denials should be unusual. A reasonable denial would include the following situations:

- Specific work papers requested contain confidential litigation matters such as criminal referrals.
- Litigation against the auditor is pending or contemplated.

Finally, to obtain access to work papers, the auditor must sign a statement of consent to the Prohibition of Disclosure or Release notice.

### Prohibition of Disclosure or Release

The report of examination, regulatory correspondence, and examination work papers are the property of OTS. OTS makes documents available to the independent audit firm for its confidential use relating to its audit of the savings association engaging the audit firm. Neither the audit firm nor any of its employees may disclose or make these documents, or any portion of them, public in any manner.

If an external auditor receives a subpoena or any legal process calling for the production of any OTS documents held by the auditor, the auditor must notify the Regional Director immediately. You should advise the attorney and, if necessary, the court of the above prohibition and refer them to § 510.5 of the OTS regulations.

## REFERENCES

## Code of Federal Regulations (12 CFR)

*FDIC Regulations*

Part 363                      Annual Independent Audits and Reporting Requirements

*OTS Regulations*

Part 510                      Miscellaneous Organizational Regulations

§ 562.4                      Audit of Savings Associations and Savings Association Holding Companies

§ 563.170(a)                Examinations and Audits

§ 563.180                    Suspicious Activity Reports and Other Reports and Statements

Part 563c                    Accounting Requirements

## United States Code (12 USC)

§ 1817(a)                    Report to Independent Auditor

## FFIEC Guidance

Interagency Policy Statement on External Auditing Programs of Banks and Savings Associations (September 22, 1999)

## American Institute of Certified Public Accountants (AICPA)

*Statement on Auditing Standards (SAS)*

No. 54                      Illegal Acts by Clients (AU 317)

No. 55                      Consideration of Internal Control in a Financial Statement Audit (AU 319)

No. 58                      Reports on Audited Financial Statements (AU 508)

No. 60                      Communication of Internal Control Structure Related Matters Noted in an Audit (AU 325)

No. 61                      Communication With Audit Committees (AU 380)

- No. 69 The Meaning of Present Fairly in Conformity with Generally Accepted Accounting Principles in the Independent Auditor's Report (AU 411)
- No. 70 Reports on the Processing of Transactions by Service Organizations (AU 324)
- No. 71 Interim Financial Information (AU 722)
- No. 79 Amendment to Statement on Auditing Standards No. 58, Reports on Audited Financial Statements (AU 508)
- No. 82 Consideration of Fraud in a Financial Statement Audit (AU 316)
- No. 89 Audit Adjustments (AU 420)
- No. 90 Audit Committee Communications (AU 380)
- No. 93 Omnibus Statement on Auditing Standards (AU 315)
- No. 94 The Effect of Information Technology on the Auditor's Consideration of Internal Control in a Financial Statement Audit (AU 319)
- No. 96 Audit Documentation

*Statement on Standards for Attestation Engagements (SSAE)*

- No. 2 Reporting on an Entity's Internal Control Structure Over Financial Reporting (AT 400)
- No. 3 Compliance Attestation (AT 500)
- No. 4 Agreed-Upon Procedures Engagement (AT 600)
- No. 6 Reporting on an Entity's Internal Control Over Financial Reporting: An Amendment to Statement on Standards for Attestation Engagements No. 2 (AT 400)
- No. 9 Amendments to Statement on Standards for Attestation Engagements Nos. 1, 2, and 3 (AT 100, 400, and 500)
- No. 10 Attestation Standards: Revision and Recodification (AT 101), supercedes SSAE Nos. 1 through 9

*AICPA Code of Professional Conduct (ET)*

Sec. 100	Independence, Integrity, and Objectivity
Sec. 100.15	Extended Audit Services (101-13)
Sec. 191	Ethics Rulings on Independence, Integrity, and Objectivity
Sec. 191.206	Member Providing Attest Report on Internal Controls (103)
Sec. 191.208	Member Providing Operational Auditing Services (104)
Sec. 191.210	Frequency of Performance of Extended Audit Procedures (105)

# External Audit Program

---

## EXAMINATION OBJECTIVES

To determine how audit procedures, findings, and recommendations affect the scope of the planned examination.

To evaluate how much the examiner can rely on the audit work to limit or supplement the examination scope.

To communicate with auditors to obtain a better understanding of high-risk or complex activities of the association.

To ensure that the auditor met regulatory requirements in the preparation and presentation of the audit report.

To determine if the association corrected deficiencies noted by the auditors.

To determine that the auditor's client is the board of directors and not management.

## MONITORING AND EXAMINATION PROCEDURES

### LEVEL I

WKP. REF.

#### Supervisory Monitoring Procedures (Examination managers)

1. Obtain copies of the audit report, report on system of internal control (report on internal control), engagement letter, audited financial statements, Securities and Exchange Commission (SEC) filings, and any other audit-related reports the regional office receives. (Also obtain a copy of all comments pertaining to any supervisory or compliance reviews performed by the regional accountant.)

Determine the type of opinion (unqualified, qualified, adverse, or disclaimer) rendered by the external auditor. If the external auditor rendered other than an unqualified opinion, find out why.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# External Audit Program

---

WKP. REF.

2. Read the reports for supervisory issues (at a minimum, verify that the regulatory capital figures in the footnotes to the audited financial statements agree with the Thrift Financial Report (TFR) for the same period).
  - Complete the [Audit-Related Report checklist in Appendix A](#) for audit-related reports.

---
3. Determine whether any identified supervisory concerns require immediate follow-up. If not, use the checklists to document needed follow-up by examination personnel.
  - Determine if there are any material weaknesses in internal control. Discuss any communication of weaknesses between management and the external auditor.

---
4. Determine whether any supervisory concerns have subsequently been reported in the association's TFR or the examination.

---
5. Update the regulatory profile for any identified supervisory concerns.

---

## Examination Planning Procedures

6. Obtain the examination file copy of the Audit-Related Report checklist prepared since the last examination.
  - Review the checklist for any documented supervisory concerns.
  - Schedule field examination follow-up on documented supervisory concerns.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



# External Audit Program

---

WKP. REF.

7. Make inquiries of association management and the external auditor to determine whether the external auditor performed any special reviews of specific departments or areas of the association since the previous examination that the association did not supply to OTS.

- Obtain copies of the reports and discuss any supervisory concerns with the auditor and management.
  - Complete the Audit-Related Report checklist.
  - Update the regulatory profile for any identified supervisory concerns and required examination follow-up.
- 

8. Determine whether you can use the audit to supplement the examination procedures.

- Review the audit work papers to identify areas where the audit work can supplement examination procedures.
  - Identify audit work that you can rely on to limit examination procedures, keeping in mind the limitations on relying on audit work.
  - Consider the auditor's competence, integrity, independence, and knowledge of regulatory matters (consult the regional accountant).
  - Determine if the institution prepared a management report, and review management's assessment of the effectiveness of internal control structures and procedures as of the end of the fiscal year, and its compliance with laws and regulations during the year.
  - Determine if the external auditor has examined, attested to, or reported separately on management's assertions concerning the internal control structure for financial reporting.
  - Consider having the auditor perform specific procedures. (This request should coincide with the auditor's normal annual audit work whenever possible.)
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# External Audit Program

---

WKP. REF.

## Examination Field Procedures

9. Perform recommended follow-up for all items as indicated in the regulatory profile and the Audit-Related Report checklist.

- 
10. Review the preceding report of examination and all external audit-related exceptions noted and determine whether management has taken appropriate corrective action.

- 
11. Discuss matters of supervisory concern and material transactions that require complex analysis with the external auditor.

- 
12. Ask association management and the external auditor about any account adjustments resulting from the most recent audit.

- Obtain a schedule of the adjustments.
- Review the adjustments to identify entries that indicate poor accounting records or controls.
- Review the adjustments to determine whether management has given appropriate attention to the affected areas and to determine whether management reported the adjustments on the TFR in the appropriate period. *Do not require restatement of the TFR unless the error is material. An error is material if it is related to a failure of a capital requirement, a change in a PCA category, a change in a component rating, or has significance for regulatory reporting purposes.*

- 
13. Review Level II procedures and perform those necessary to test, support, and present examination conclusions derived from performing Level I procedures.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# External Audit Program

---

WKP. REF.

## LEVEL II

### Examination Field Procedures

1. If you plan a review of the audit work papers, arrange for the auditor to make the work papers available at the association's office. Only sign a document to acknowledge receipt of the copies of the work papers. (Alternatively, the accountant may request that you review the work papers in the auditor's office.)
    - Gather evidence on identified matters as necessary to substantiate stated examination objectives.
    - Prepare a list of work papers to copy, if needed.
    - Submit the list to the auditor and obtain a firm commitment on the delivery date, if needed.
    - Determine whether work papers support conclusions by the external auditor.
    - Modify the examination scope as considered necessary.
    - If there are questions or concerns about the application of generally accepted accounting principles or generally accepted auditing standards based on the work paper review, consult the regional accountant.
- 
2. Assess the CPA's independence and competence.
    - Evaluate the independence, objectivity, and competence of those providing the external audit.
    - Determine if the institution has recently changed auditors. If so, discuss the reason for the change.
    - Make inquiries of the appropriate association officials concerning their knowledge of any improper relationship (stockholder, significant unsecured borrower, officer, or director) or business affiliations with the CPA.
    - Obtain and review loan listings, contracts, and stockholder listings to substantiate representations of independence, if circumstances warrant.

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# External Audit Program

---

WKP. REF.

- Determine that the audit committee of the board of directors verified that the audit engagement staff was independent and competent to audit the association.
  - Determine that the outside directors on the audit committee monitor the relationship between the auditor and management. The auditor works for the board of directors, not management. The auditor should not be an advocate for management.
- 
3. Review and determine whether the board of directors or its audit committee at least annually reviews and approves any policies pertaining to the institution's external audit function.
- 
4. Meet with the external auditor to discuss significant audit findings.
- 
5. Ensure that your review meets the Objectives of this Handbook Section. State your findings and conclusions, and appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.
- 

## EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

### Audit-Related Report Checklist

Association		Docket #
Year End	Type of Report(s)	
Audit Firm	Office	

*Instructions:* The examination manager is responsible for the review of all audit-related reports required by 12 CFR § 562.4 and FDIC Part 363. Audit-related reports include report of audit, audited financial statements, reports on internal control, the management report on internal control, the accountant's attestation report, and special agreed-upon procedures reports. Use this checklist to describe information of a supervisory nature and to communicate any supervisory follow-up to examiners. You may use one or more checklists for each annual audit. If immediate follow-up is not necessary, place this checklist in the examination file for follow-up by examiners in the next examination. You must complete this checklist within 90 days of receipt of the audit-related report. This checklist is optional for reports filed with OTS on a voluntary basis. File completed checklists in the supervisory file. *Document all responses on this checklist with attachments as needed.*

1. Assemble the most recent report of examination, thrift financial report, other regulatory reports, audited financial statements, and other audit-related reports.
2. Scan the report under review and note items of supervisory interest, such as, new line items or footnotes in audited financial statements that indicate a new type of transaction or exposure area for the association; material weaknesses reported in the system of internal control, etc.
3. Review the other documents assembled under item 1 above and note the extent of any OTS knowledge of the supervisory items identified in item 2 above.
4. Document required follow-up for items of supervisory concern.
5. Update the regulatory profile to reflect key audit information and any safety and soundness concerns.
6. Attach this questionnaire to the supervisory file copy and examination file copy of the audit report under review.

Reviewed by	Date
Follow-up completed by	Date
Examination Manager Approval	Date

**This page intentionally left blank**

**Comparison of OTS and FDIC Annual External Audit Requirements**

**OTS 12 CFR 562.4**

**FDIC 12 CFR Part 363**

<b>Scope</b>		
	<p>The OTS requires an external audit for safety and soundness purposes if a savings association has received a composite rating of 3, 4, or 5 under UFIRS. [12 CFR 562.4(a) and (b)(1)]</p> <p>The Director may waive the external audit requirement for a saving association if the Director determines that an audit would not provide further information on safety and soundness issues relevant to examination rating. [12 CFR 562.4(c)(2)]</p> <p>The OTS requires an external audit for a savings and loan holding company that controls savings association subsidiary(ies) with aggregate consolidated assets of \$500 million or more. [12 CFR 562.4(b)(2)]</p> <p>A savings association holding company may request a modification or waiver of the external audit requirement. [Handbook - Section 350; paragraph heading ‘OTS Required Audit: Audit of Savings Association Holding Companies with \$500 Million or More of Total Assets; Modification or Waiver’]</p> <p>The audited consolidated financial statement of the savings association holding company will be accepted in lieu of separate audited financial statements of the savings association. [Handbook - Section 350; paragraph heading ‘OTS Required Audit: Audit of Savings Associations that Receive a Composite CAMELS Rating of 3, 4, or 5; Required Reports’]</p>	<p>Insured depository institutions, including savings associations, with total assets of \$500 million or more at the beginning of each fiscal year after December 31, 1992. [12 CFR 363.1(a)]</p> <p>The audited financial statements (AFS) requirement may be satisfied by audited financial statements of the consolidated holding company. All other requirements of Part 363 may be satisfied at the holding company level if certain conditions are met. [12 CFR 363.1(b)]</p>

**OTS 12 CFR 562.4**

**FDIC 12 CFR Part 363**

<b>Auditing Standard</b>	Generally accepted auditing standards (GAAS).	GAAS and the standards of section 37 of the Federal Deposit Insurance Act (FDIA). [12 CFR 363.3(a)]
<b>Qualifications for Auditors</b>	<p>Certified public accountant (CPA) who is independent by AICPA and SEC standards and is enrolled in an FDIC-approved peer review program. CPA agrees in the engagement letter to provide OTS with access to and copies of any work paper, policies, and procedures relating to the services performed. [12 CFR 562.4(d)(1), (2), (3), and (4)]</p> <p>For voluntary audits the CPA does not have to be enrolled in a peer review program. [12 CFR 562.4(e)]</p>	<p>CPA who is independent by AICPA and SEC approved peer review program. [12 CFR 363 Appendix (13), (14), and (15)]</p>
<p><b>Filing and Notice Requirements</b>  <b>a) Savings Association</b></p>	<p>A savings association that is required to obtain an external audit for safety and soundness reasons should submit two copies to the Regional Director of the following: the audited financial statements, any reports from the CPA that make reference to the external audit, and other OTS requested supplemental information, or schedules. The required reports shall be forwarded to the Regional Director within 90 days of the fiscal year-end or within 15 days of receipt, whichever is earlier.</p>	<p>When an audit is required the FDIC requires the following reports:</p> <ul style="list-style-type: none"> <li>• AFS prepared in accordance with generally accepted accounting principles (GAAP).</li> <li>• Audit Opinion on AFS.</li> <li>• Management Report:             <ul style="list-style-type: none"> <li>— Statement of responsibility</li> <li>— Assessment of effectiveness of the internal control structure over financial reporting, and</li> <li>— Assessment of compliance with designated safety and soundness laws and regulations.</li> </ul> </li> <li>• Accountant’s attestation report on management’s assessment of effectiveness of internal control structure.</li> <li>• Any management letter, qualification, or other report(s) issued by the accountant relating to services provided pursuant to 12 CFR Part 363.</li> </ul>



**OTS 12 CFR 562.4**

**FDIC 12 CFR Part 363**

<p><b>Filing and Notice Requirements</b>  <b>a) Savings Association</b>  <i>(continued)</i></p>	<p>When a savings association has assets of \$500 million or more, it will instead file with the FDIC and OTS the reports required pursuant to FDIC Regulation Part 363 and FDIC guidelines at Appendix A to Part 363. [Handbook - Section 350; paragraph heading ‘External Audits’]</p> <p>A savings association holding company should comply with the reporting requirements at item 21, “Financial Statements” in the H-(b)21 Annual Report. [Handbook - Section 350; paragraph heading ‘Savings Association Holding Companies with \$500 Million or More of Total Assets’]</p> <p>Institutions that obtain voluntary audits are not required to file any reports or notices with the OTS.</p>	
<p><b>Audit Waivers</b></p>	<p>The savings association may make a written request for a waiver from the OTS safety and soundness audit requirement. OTS will waive the audit requirement if it determines that an audit is not the most effective means to address safety and soundness concerns that caused the composite CAMELS rating of 3, 4, or 5. [Handbook - Section 350; paragraph heading ‘Written Request for Waiver of External Audit Agreement’]</p> <p>A savings association holding company may request a modification or waiver of the external audit requirement. [Handbook - Section 350; paragraph heading ‘Savings Association Holding Companies with \$500 Million or More of Total Assets; Safety and Soundness Considerations for Granting Waiver Requests’]</p>	<p>No similar provision.</p>

OTS 12 CFR 562.4FDIC 12 CFR Part 363

<b>Filing and Notice Requirements</b> <b>b) Auditors</b>	No requirement to provided notice of change in auditors (the FDIC has a notice requirement for institutions with \$500 million or more in assets).	Notice of engagement or change of accountant. [12 CFR 363.4]
	Make the peer review report available to examiner during examination, do not forward to OTS. [Handbook - Section 350; paragraph heading 'Auditor Requirements For Required Audit or Required Agreed-Upon Procedures']	Notice of termination of accountant. Peer Review Report. [12 CFR 363.3(c) and Statute]
<b>Audit Committee Requirements</b>	None	Must consist of members of the board who are independent of management <sup>1</sup> .  [12 CFR 363 Appendix (28) and (29)]  Institutions with assets of \$3 billion or more must have access to outside counsel and include members with banking and financial management expertise who are not large customers of the institution.
<b>Documentation and Other Considerations for Audit Work Papers</b>	The CPA agrees in the engagement letter (do not forward engagement letter to OTS) to provide OTS with access to and copies of any work papers, policies, and procedures relating to services performed. [12 CFR 562.4(d)(2)]	Copies of any work papers, policies, and procedures relating to services performed under 12 CFR 363 must be provided upon request. [12 CFR 363 Appendix (13)]  Peer review work papers must be retained for 120 days after peer review report is filed with FDIC. [12 CFR 363 Appendix (15(c))]

<sup>1</sup> Members of the holding company's audit committee may serve as the audit committee of any subsidiary institution if they are otherwise independent of management of the subsidiary.  
[12 CFR 363 Appendix (31)]

---

**FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL**  
**INTERAGENCY POLICY STATEMENT ON EXTERNAL AUDITING PROGRAMS OF BANKS**  
**AND SAVINGS ASSOCIATIONS**

## INTRODUCTION

The board of directors and senior managers of a banking institution or savings association (institution) are responsible for ensuring that the institution operates in a safe and sound manner. To achieve this goal and meet the safety and soundness guidelines implementing Section 39 of the Federal Deposit Insurance Act (FDI Act) (12 U.S.C. § 1831p-1),<sup>1</sup> the institution should maintain effective systems and internal control<sup>2</sup> to produce reliable and accurate financial reports.

Accurate financial reporting is essential to an institution's safety and soundness for numerous reasons. First, accurate financial information enables management to effectively manage the institution's risks and make sound business decisions. In addition, institutions are required by law<sup>3</sup> to provide accurate and timely financial reports (e.g., Reports of Condition and Income [Call Reports] and Thrift Financial Reports) to their appropriate regulatory agency. These reports serve an important role in the agencies'<sup>4</sup> risk-focused supervision programs by contributing to their pre-examination planning, off-site monitoring programs, and assessments of an institution's capital adequacy and financial strength. Further, reliable financial reports are necessary for the institution to raise capital. They provide data to stockholders, depositors and other funds providers, borrowers, and potential investors on the company's financial position and results of operations. Such information is critical to effective market discipline of the institution.

To help ensure accurate and reliable financial reporting, the agencies recommend that the board of directors of each institution establish and maintain an external auditing program. An external auditing program should be an important component of an institution's overall risk management process. For example, an external auditing program complements the internal auditing function of an institution by providing management and the board of directors with an independent and objective view of the reliability of the institution's financial statements and the adequacy of its financial reporting internal controls. Additionally, an effective external auditing program contributes to the efficiency of the agencies' risk-focused examination process. By considering the significant risk areas of an institution, an effective external auditing program may reduce the examination time the agencies spend in such areas. Moreover, it can improve the safety and soundness of an institution substantially and lessen the risk the institution poses to the insurance funds administered by the Federal Deposit Insurance Corporation (FDIC).

This policy statement outlines the characteristics of an effective external auditing program and provides examples of how an institution can use an external auditor to help ensure the reliability of its financial reports. It also provides guidance on how an examiner may assess an institution's external auditing program. In addition, this policy statement provides specific guidance on external auditing programs for institutions that are holding company subsidiaries, newly insured institutions, and institutions presenting supervisory concerns.

The adoption of a financial statement audit or other specified type of external auditing program is generally only required in specific circumstances. For example, insured depository institutions covered by Section 36

---

<sup>1</sup> See 12 CFR Part 30 for national banks; 12 CFR Part 364 for state nonmember banks; 12 CFR Part 208 for state member banks; and 12 CFR Part 510 for savings associations.

<sup>2</sup> This Policy Statement provides guidance consistent with the guidance established in the "Interagency Policy Statement on the Internal Audit Function and its Outsourcing."

<sup>3</sup> See 12 USC 161 for national banks; 12 USC 1817a for state nonmember banks, 12 USC 324 for state member banks; and 12 USC 1464(v) for savings associations.

<sup>4</sup> Terms defined in Appendix A are italicized the first time they appear in this policy statement.

---

of the FDI Act (12 U.S.C. § 1831m), as implemented by Part 363 of the FDIC's regulations (12 CFR part 363), are required to have an external audit and an audit committee. Therefore, this policy statement is directed toward banks and savings associations which are exempt from Part 363 (i.e., institutions with less than \$500 million in total assets at the beginning of their fiscal year) or are not otherwise subject to audit requirements by order, agreement, statute, or agency regulations.

## OVERVIEW OF EXTERNAL AUDITING PROGRAMS

### Responsibilities of the Board of Directors

The board of directors of an institution is responsible for determining how to best obtain reasonable assurance that the institution's financial statements and regulatory reports are reliably prepared. In this regard, the board is also responsible for ensuring that its external auditing program is appropriate for the institution and adequately addresses the financial reporting aspects of the significant risk areas and any other areas of concern of the institution's business.

To help ensure the adequacy of its internal and external auditing programs, the agencies encourage the board of directors of each institution that is not otherwise required to do so to establish an audit committee consisting entirely of outside directors.<sup>5</sup> However, if this is impracticable, the board should organize the audit committee so that outside directors constitute a majority of the membership.

### Audit Committee

The audit committee or board of directors is responsible for identifying at least annually the risk areas of the institution's activities and assessing the extent of external auditing involvement needed over each area. The audit committee or board is then responsible for determining what type of external auditing program will best meet the institution's needs (refer to the descriptions under "Types of External Auditing Programs").

When evaluating the institution's external auditing needs, the board or audit committee should consider the size of the institution and the nature, scope, and complexity of its operations. It should also consider the potential benefits of an audit of the institution's financial statements or an examination of the institution's internal control structure over financial reporting, or both. In addition, the board or audit committee may determine that additional or specific external auditing procedures are warranted for a particular year or several years to cover areas of particularly high risk or special concern. The reasons supporting these decisions should be recorded in the committee's or board's minutes.

If, in its annual consideration of the institution's external auditing program, the board or audit committee determines, after considering its inherent limitations, that an agreed-upon procedures/state-required examination is sufficient, they should also consider whether an independent public accountant should perform the work. When an independent public accountant performs auditing and attestation services, the accountant must conduct his or her work under, and may be held accountable for departures from, professional standards. Furthermore, when the external auditing program includes an audit of the financial statements, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial statements are presented fairly, in all material respects, in accordance with generally accepted accounting principles (GAAP). When the external auditing program includes an examination of the internal control structure over financial reporting, the board or audit committee obtains an opinion from the independent public accountant stating whether the financial reporting process is subject to any material weaknesses.

---

<sup>5</sup> Institutions with \$500 million or more in total assets must establish an independent audit committee made up of outside directors who are independent of management. See 12 U.S.C. 1831m(g)(1) and 12 CFR 363.5.

---

Both the staff performing an internal audit function and the independent public accountant or other external auditor should have unrestricted access to the board or audit committee without the need for any prior management knowledge or approval. Other duties of an audit committee may include reviewing the independence of the external auditor annually, consulting with management, seeking an opinion on an accounting issue, and overseeing the quarterly regulatory reporting process. The audit committee should report its findings periodically to the full board of directors.

## **EXTERNAL AUDITING PROGRAMS**

### Basic Attributes

External auditing programs should provide the board of directors with information about the institution's financial reporting risk areas, e. g., the institution's internal control over financial reporting, the accuracy of its recording of transactions, and the completeness of its financial reports prepared in accordance with GAAP.

The board or audit committee of each institution at least annually should review the risks inherent in its particular activities to determine the scope of its external auditing program. For most institutions, the lending and investment securities activities present the most significant risks that affect financial reporting. Thus, external auditing programs should include specific procedures designed to test at least annually the risks associated with the loan and investment portfolios. This includes testing of internal control over financial reporting, such as management's process to determine the adequacy of the allowance for loan and lease losses and whether this process is based on a comprehensive, adequately documented, and consistently applied analysis of the institution's loan and lease portfolio.

An institution or its subsidiaries may have other significant financial reporting risk areas such as material real estate investments, insurance underwriting or sales activities, securities broker-dealer or similar activities (including securities underwriting and investment advisory services), loan servicing activities, or fiduciary activities. The external auditing program should address these and other activities the board or audit committee determines present significant financial reporting risks to the institution.

### Types of External Auditing Programs

The agencies consider an annual audit of an institution's financial statements performed by an independent public accountant to be the preferred type of external auditing program. The agencies also consider an annual examination of the effectiveness of the internal control structure over financial reporting or an audit of an institution's balance sheet, both performed by an independent public accountant, to be acceptable alternative external auditing programs. However, the agencies recognize that some institutions only have agreed-upon procedures/state-required examinations performed annually as their external auditing program. Regardless of the option chosen, the board or audit committee should agree in advance with the external auditor on the objectives and scope of the external auditing program.

*FINANCIAL STATEMENT AUDIT BY AN INDEPENDENT PUBLIC ACCOUNTANT.* The agencies encourage all institutions to have an external audit performed in accordance with generally accepted auditing standards (GAAS). The audit's scope should be sufficient to enable the auditor to express an opinion on the institution's financial statements taken as a whole.

A financial statement audit provides assurance about the fair presentation of an institution's financial statements. In addition, an audit may provide recommendations for management in carrying out its control responsibilities. For example, an audit may provide management with guidance on establishing or improving accounting and operating policies and recommendations on internal control (including internal auditing programs) necessary to ensure the fair presentation of the financial statements.

*REPORTING BY AN INDEPENDENT PUBLIC ACCOUNTANT ON AN INSTITUTION'S INTERNAL CONTROL STRUCTURE OVER FINANCIAL REPORTING.* Another external auditing program is an independent public accountant's examination and report on management's assertion on the effectiveness of the institution's internal control over financial reporting. For a smaller institution with less complex operations, this type of engagement is likely to be less costly than an audit of its financial statements or its balance sheet. It would specifically provide recommendations for improving internal control, including suggestions for compensating controls, to mitigate the risks due to staffing and resource limitations.

Such an attestation engagement may be performed for all internal controls relating to the preparation of annual financial statements or specified schedules of the institution's regulatory reports.<sup>6</sup> This type of engagement is performed under generally accepted standards for attestation engagements (GASAE).<sup>7</sup>

*BALANCE SHEET AUDIT PERFORMED BY AN INDEPENDENT PUBLIC ACCOUNTANT.* With this program, the institution engages an independent public accountant to examine and report only on the balance sheet. As with the audit of the financial statements, this audit is performed in accordance with GAAS. The cost of a balance sheet audit is likely to be less than a financial statement audit. However, under this type of program, the accountant does not examine or report on the fairness of the presentation of the institution's income statement, statement of changes in equity capital, or statement of cash flows.

*AGREED-UPON PROCEDURES/STATE-REQUIRED EXAMINATIONS.* Some state-chartered depository institutions are required by state statute or regulation to have specified procedures performed annually by their directors or independent persons.<sup>8</sup> The bylaws of many national banks also require that some specified procedures be performed annually by directors or others, including internal or independent persons. Depending upon the scope of the engagement, the cost of agreed-upon procedures or a state-required examination may be less than the cost of an audit. However, under this type of program, the independent auditor does not report on the fairness of the institution's financial statements or attest to the effectiveness of the internal control structure over financial reporting. The findings or results of the procedures are usually presented to the board or the audit committee so that they may draw their own conclusions about the quality of the financial reporting or the sufficiency of internal control.

When choosing this type of external auditing program, the board or audit committee is responsible for determining whether these procedures meet the external auditing needs of the institution, considering its size and the nature, scope, and complexity of its business activities. For example, if an institution's external auditing

<sup>6</sup> Since the lending and investment securities activities generally present the most significant risks that affect an institution's financial reporting, management's assertion and the accountant's attestation generally should cover those regulatory report schedules. If the institution has trading or off-balance sheet activities that present material financial reporting risks, the board or audit committee should ensure that the regulatory report schedules for those activities also are covered by management's assertion and the accountant's attestation. For banks and savings associations, the lending, investment securities, trading, and off-balance sheet schedules consist of:

<u>Area</u>	<u>Reports of Condition and Income Schedules</u>	<u>Thrift Financial Report Schedules</u>
Loans and Lease Financing Receivables	RC-C, Part I	SC, CF
Past Due and Nonaccrual Loans, Leases, and Other Assets	RC-N	PD
Allowance for Credit Losses	RI-B	SC, VA
Securities	RC-B	SC, SI, CF
Trading Assets and Liabilities	RC-D	SO, SI
Off-Balance Sheet Items	RC-L	SI, CMR

These schedules are not intended to address all possible risks in an institution.

<sup>7</sup> An attestation engagement is not an audit. It is performed under different professional standards than an audit of an institution's financial statements or its balance sheet.

<sup>8</sup> When performed by an independent public accountant, "specified procedures" and "agreed-upon procedures" engagements are performed under standards, which are different professional standards than those used for an audit of an institution's financial statements or its balance sheet.

program consists solely of confirmations of deposits and loans, the board or committee should consider expanding the scope of the auditing work performed to include additional procedures to test the institution's high risk areas. Moreover, a financial statement audit, an examination of the effectiveness of the internal control structure over financial reporting, and a balance sheet audit may be accepted in some states and for national banks in lieu of agreed-upon procedures/state-required examinations.

#### Other Considerations

*TIMING.* The preferable time to schedule the performance of an external auditing program is as of an institution's fiscal year-end. However, a quarter-end date that coincides with a regulatory report date provides similar benefits. Such an approach allows the institution to incorporate the results of the external auditing program into its regulatory reporting process and, if appropriate, amend the regulatory reports.

*EXTERNAL AUDITING STAFF.* The agencies encourage an institution to engage an independent public accountant to perform its external auditing program. An independent public accountant provides a nationally recognized standard of knowledge and objectivity by performing engagements under GAAS or GASAE. The firm or independent person selected to conduct an external auditing program and the staff carrying out the work should have experience with financial institution accounting and auditing or similar expertise and should be knowledgeable about relevant laws and regulations.

### **SPECIAL SITUATIONS**

#### Holding Company Subsidiaries

When an institution is owned by another entity (such as a holding company), it may be appropriate to address the scope of its external audit program in terms of the institution's relationship to the consolidated group. In such cases, if the group's consolidated financial statements for the same year are audited, the agencies generally would not expect the subsidiary of a holding company to obtain a separate audit of its financial statements. Nevertheless, the board of directors or audit committee of the subsidiary may determine that its activities involve significant risks to the subsidiary that are not within the procedural scope of the audit of the financial statements of the consolidated entity. For example, the risks arising from the subsidiary's activities may be immaterial to the financial statements of the consolidated entity, but material to the subsidiary. Under such circumstances, the audit committee or board of the subsidiary should consider strengthening the internal audit coverage of those activities or implementing an appropriate alternative external auditing program.

#### Newly Insured Institutions

Under the FDIC Statement of Policy on Applications for Deposit Insurance, applicants for deposit insurance coverage are expected to commit the depository institution to obtain annual audits by an independent public accountant once it begins operations as an insured institution and for a limited period thereafter.

#### Institutions Presenting Supervisory Concerns

As previously noted, an external auditing program complements the agencies' supervisory process and the institution's internal auditing program by identifying or further clarifying issues of potential concern or exposure. An external auditing program also can greatly assist management in taking corrective action, particularly when weaknesses are detected in internal control or management information systems affecting financial reporting.

---

The agencies may require a financial institution presenting safety and soundness concerns to engage an independent public accountant or other independent external auditor to perform external auditing services.<sup>9</sup> Supervisory concerns may include:

- Inadequate internal control, including the internal auditing program;
- A board of directors generally uninformed about internal control;
- Evidence of insider abuse;
- Known or suspected defalcations;
- Known or suspected criminal activity;
- Probable director liability for losses;
- The need for direct verification of loans or deposits;
- Questionable transactions with affiliates; or
- The need for improvements in the external auditing program.

The agencies may also require that the institution provide its appropriate supervisory office with a copy of any reports, including management letters, issued by the independent public accountant or other external auditor. They also may require the institution to notify the supervisory office prior to any meeting with the independent public accountant or other external auditor at which auditing findings are to be presented.

## **EXAMINER GUIDANCE**

### Review of the External Auditing Program

The review of an institution's external auditing program is a normal part of the agencies' examination procedures. An examiner's evaluation of, and any recommendations for improvements in, an institution's external auditing program will consider the institution's size; the nature, scope, and complexity of its business activities; its risk profile; any actions taken or planned by it to minimize or eliminate identified weaknesses; the extent of its internal audit program; and any compensating controls in place. Examiners will exercise judgment and discretion in evaluating the adequacy of an institution's external auditing program.

Specifically, examiners will consider the policies, processes, and personnel surrounding an institution's external auditing program in determining whether:

- The board of directors or its audit committee adequately reviews and approves external auditing program policies at least annually.
- The external auditing program is conducted by an independent public accountant or other independent auditor and is appropriate for the institution.
- The engagement letter covering external auditing activities is adequate.
- The report prepared by the auditor on the results of the external auditing program adequately explains the auditor's findings.

---

<sup>9</sup> The Office of Thrift Supervision requires an external audit by an independent public accountant for savings associations with a composite rating of 3, 4, or 5 under the Uniform Financial Institution Rating System, and on a case-by-case basis.



- 
- The external auditor maintains appropriate independence regarding relationships with the institution under relevant professional standards.
  - The board of directors performs due diligence on the relevant experience and competence of the independent auditor and staff carrying out the work (whether or not an independent public accountant is engaged).
  - The board or audit committee minutes reflect approval and monitoring of the external auditing program and schedule, including board or committee reviews of audit reports with management and timely action on audit findings and recommendations.

#### Access to Reports

Management should provide the independent public accountant or other auditor with access to all examination reports and written communication between the institution and the agencies or state bank supervisor since the last external auditing activity. Management also should provide the accountant with access to any supervisory memoranda of understanding, written agreements, administrative orders, reports of action initiated or taken by a federal or state banking agency under section 8 of the FDI Act (or a similar state law), and proposed or ordered assessments of civil money penalties against the institution or an institution-related party, as well as any associated correspondence. The auditor must maintain the confidentiality of examination reports and other confidential supervisory information.

In addition, the independent public accountant or other auditor of an institution should agree in the engagement letter to grant examiners access to all the accountant's or auditor's work papers and other material pertaining to the institution prepared in the course of performing the completed external auditing program.

Institutions should provide reports<sup>10</sup> issued by the independent public accountant or other auditor pertaining to the external auditing program, including any management letters, to the agencies and any state authority in accordance with their appropriate supervisory office's guidance.<sup>11</sup> Significant developments regarding the external auditing program should be communicated promptly to the appropriate supervisory office. Examples of those developments include the hiring of an independent public accountant or other third party to perform external auditing work and a change in, or termination of, an independent public accountant or other external auditor.

### **Appendix A – Definitions**

*Agencies.* The agencies are the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS).

*Appropriate supervisory office.* The regional or district office of the institution's primary federal banking agency responsible for supervising the institution or, in the case of an institution that is part of a group of related insured institutions, the regional or district office of the institution's federal banking agency responsi-

---

<sup>10</sup> The institution's engagement letter is not a "report" and is not expected to be submitted to the appropriate supervisory office unless specifically requested by that office.

<sup>11</sup> When an institution's financial information is included in the audited consolidated financial statements of its parent company, the institution should provide a copy of the audited financial statements of the consolidated company and any other reports by the independent public accountant in accordance with their appropriate supervisory office's guidance. If several institutions are owned by one parent company, a single copy of the reports may be supplied in accordance with the guidance of the appropriate supervisory office of each agency supervising one or more of the affiliated institutions and the holding company. A transmittal letter should identify the institutions covered. Any notifications of changes in, or terminations of, a consolidated company's independent public accountant may be similarly supplied to the appropriate supervisory office of each supervising agency.

ble for monitoring the group. If the institution is a subsidiary of a holding company, the term “appropriate supervisory office” also includes the federal banking agency responsible for supervising the holding company. In addition, if the institution is state-chartered, the term “appropriate supervisory office” includes the appropriate state bank or savings association regulatory authority.

*Audit.* An examination of the financial statements, accounting records, and other supporting evidence of an institution performed by an independent certified or licensed public accountant in accordance with generally accepted auditing standards (GAAS) and of sufficient scope to enable the independent public accountant to express an opinion on the institution’s financial statements as to their presentation in accordance with generally accepted accounting principles (GAAP).

*Audit committee.* A committee of the board of directors whose members should, to the extent possible, be knowledgeable about accounting and auditing. The committee should be responsible for reviewing and approving the institution’s internal and external auditing programs or recommending adoption of these programs to the full board.

*Balance sheet audit performed by an independent public accountant.* An examination of an institution’s balance sheet and any accompanying footnotes performed and reported on by an independent public accountant in accordance with GAAS and of sufficient scope to enable the independent public accountant to express an opinion on the fairness of the balance sheet presentation in accordance with GAAP.

*Engagement letter.* A letter from an independent public accountant to the board of directors or audit committee of an institution that usually addresses the purpose and scope of the external auditing work to be performed, period of time to be covered by the auditing work, reports expected to be rendered, and any limitations placed on the scope of the auditing work.

*Examination of the internal control structure over financial reporting.* See Reporting by an Independent Public Accountant on an Institution’s Internal Control Structure Over Financial Reporting.

*External auditing program.* The performance of procedures to test and evaluate high risk areas of a institution’s business by an independent auditor, who may or may not be a public accountant, sufficient for the auditor to be able to express an opinion on the financial statements or to report on the results of the procedures performed.

*Financial statement audit by an independent public accountant.* See Audit.

*Financial statements.* The statements of financial position (balance sheet), income, cash flows, and changes in equity together with related notes.

*Independent public accountant.* An accountant who is independent of the institution and registered or licensed to practice, and holds himself or herself out, as a public accountant, and who is in good standing under the laws of the state or other political subdivision of the United States in which the home office of the institution is located. The independent public accountant should comply with the American Institute of Certified Public Accountants’ (AICPA) [Code of Professional Conduct](#) and any related guidance adopted by the Independence Standards Board and the agencies. No certified public accountant or public accountant will be recognized as independent who is not independent both in fact and in appearance.

*Internal auditing.* An independent assessment function established within an institution to examine and evaluate its system of internal control and the efficiency with which the various units of the institution are carrying out their assigned tasks. The objective of internal auditing is to assist the management and directors of the institution in the effective discharge of their responsibilities. To this end, internal auditing furnishes management with analyses, evaluations, recommendations, counsel, and information concerning the activities reviewed.

*Outside directors.* Members of an institution's board of directors who are not officers, employees, or principal stockholders of the institution, its subsidiaries, or its affiliates, and who do not have any material business dealings with the institution, its subsidiaries, or its affiliates.

*Regulatory reports.* These reports are the Reports of Condition and Income (Call Reports) for banks, Thrift Financial Reports (TFRs) for savings associations, Federal Reserve (FR) Y reports for bank holding companies, and the H-(b)11 Annual Report for thrift holding companies.

*Reporting by an independent public accountant on an institution's internal control structure over financial reporting.* Under this engagement, management evaluates and documents its review of the effectiveness of the institution's internal control over financial reporting in the identified risk areas as of a specific report date. Management prepares a written assertion, which specifies the criteria on which management based its evaluation about the effectiveness of the institution's internal control over financial reporting in the identified risk areas and states management's opinion on the effectiveness of internal control over this specified financial reporting. The independent public accountant is engaged to perform tests on the internal control over the specified financial reporting in order to attest to management's assertion. If the accountant concurs with management's assertion, even if the assertion discloses one or more instances of material internal control weakness, the accountant would provide a report attesting to management's assertion.

*Risk areas.* Those particular activities of an institution that expose it to greater potential losses if problems exist and go undetected. The areas with the highest financial reporting risk in most institutions generally are their lending and investment securities activities.

*Specified procedures.* Procedures agreed-upon by the institution and the auditor to test its activities in certain areas. The auditor reports findings and test results, but does not express an opinion on controls or balances. If performed by an independent public accountant, these procedures should be performed under generally accepted standards for attestation engagements (GASAE).

Dated: September 22, 1999.

**Keith Todd,**

*Executive Secretary,*

*Federal Financial Institutions Examination Council.*

**This page intentionally left blank**

**DRAFT: SAMPLE LETTER TO REQUEST AUDIT WORK PAPERS**

**Office of Thrift Supervision**  
 Department of the Treasury

1700 G Street, N.W., Washington, DC 20552 • (202) 906-6000

Mr./Ms. \_\_\_\_\_  
 Accounting Firm  
 Address  
 City, State, Zip Code

Dear Mr./Ms. \_\_\_\_\_:

The Office of Supervision (OTS) requires, under its regulation 12 CFR 562.4(d)(2), that the independent public accountant, engaged in an external audit of a savings association, agree in the engagement letter to provide OTS with access to and copies of any work papers, policies, and procedures relating to the services performed. The OTS has a program to review auditors' work papers to enhance its supervision of savings associations. The OTS has selected your client, \_\_\_\_\_ (name of institution and city), \_\_\_\_\_ for a work paper review.

Please make all the original work papers relating to the audit of this institution or its parent holding company for the year ended \_\_\_\_\_ (date) available for review. In addition to the requested work papers, we may request to review your firm's policies and procedures relating to this audit.

To limit the burden of the work paper review, we will conduct our review at a site of your choice. The review process may be expedited if an individual who is familiar with the audit is available to respond to inquiries. We have or will advise \_\_\_\_\_ (name of officer of the client institution) of \_\_\_\_\_ (name of institution) of this request.

Examiner \_\_\_\_\_ (name) at \_\_\_\_\_ (telephone number) will contact your office within the next several days to make arrangements for the review.

Sincerely,

Examiner in Charge

cc: Chief Executive Officer  
 Regional Accountant

**This page intentionally left blank**

**SAMPLE LETTER FROM ACCOUNTING FIRM**

[Letterhead of Accounting Firm]

[Date]

[Name of Regulator]

Pursuant to your responsibilities as federal regulator and examiner of (name of financial institution), you have requested copies of certain of our working papers in connection with our report on the (name of company's) financial statements for the year ending (date). The copies are identified as follows:

- (Describe the working papers)

These materials contain non-public [confidential/exempt] examination-related information under 12 C.F.R. Part 510 [or other applicable regulation] and we request that they be treated in accordance with that regulation.

[Signature of Firm Member]

**ACKNOWLEDGMENT OF RECEIPT**

[Name of Regulator]

By: \_\_\_\_\_

Date: \_\_\_\_\_

**This page intentionally left blank**



## Internal Audit

Appraising the effectiveness of an institution's internal audit function is integral to evaluating an institution's maintenance and effectiveness of internal control, and the integrity of its financial records.

Pursuant to Section 39 of the Federal Deposit Insurance Act, the interagency guidelines for safety and soundness state that each institution should have an internal audit function that is appropriate to its size and nature, and scope of its activities. All large thrifts and those with complex operations should have an internal audit function. Regardless of size, thrifts should consider the need for an internal audit function.

---

### L I N K S

---

 [Program](#)

---

 [Questionnaire](#)

---

 [Appendix A](#)

---

 [Appendix B](#)

---

A strong internal audit function should provide the following elements within the internal audit program:

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

This Section of the Handbook describes the objectives of, and the work performed by, internal auditors and offers guidelines for regulatory staff in evaluating their work. You should use it in conjunction with [Handbook Section 340, Internal Control](#).

## INTERNAL AUDIT FUNCTION

Use of an internal audit function for control and monitoring purposes is consistent with the description set forth by the Institute of Internal Auditors (IIA). The IIA's Standards for the Professional Practice of Internal Auditing state that an internal audit is:

- an independent, objective assurance and consulting activity designed to add value and improve on an organization's operations. It helps an organization accomplish its objectives by bringing a systematic disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. The practice of professional internal auditing goes beyond examining accounting controls, records, and financial statements, and reports.

A savings association's internal audit program should consist of the policies and procedures that govern its internal audit functions, including risk-based audit programs and outsourced internal audit work, if applicable. While smaller savings associations' audit programs may not be as formal as those found in larger more complex savings associations, all institutions' internal audit program should incorporate the following:

- An audit charter or mission statement that sets forth the audit department's purpose, objectives, organization, authority, and responsibilities. The charter should include a discussion about the scope of the audit committee responsibilities and how it carries out those responsibilities. The audit committee or board should periodically assess the internal audit function, and take appropriate action to ensure its ongoing reliability and effectiveness.
- An audit plan that addresses goals, schedules, staffing budget, reporting, and, if applicable, financial budgets.
- A policies and procedures manual for audit work programs and, if applicable, risk-based auditing or risk assessments and outsourcing of internal audit work.
- A program for training audit staff, including orientation and in-house and external training opportunities.
- A quality assurance program, performed by internal or external parties, to evaluate the operations of the internal audit department. This may include ongoing reviews of the performance of the internal audit activity, or periodic reviews performed through self-assessment, or by other persons within the organization with knowledge of internal auditing practices. A qualified, independent reviewer or review team outside the organization may also conduct external assessments.

Internal auditors should evaluate the efficiency and adequacy of the internal audit system, and test the continuing effectiveness and maintenance of controls. An adequate internal audit function should also incorporate the following:

- Procedures to determine the reliability of information produced within the institution and the effectiveness of internal policies and procedures. For example, internal auditors often help formulate and revise policies and procedures to plan and implement safeguards and controls, including ensuring appropriate evidence and audit trails.
- Recommendations to assist management in attaining the most efficient administration of institution operations. Internal auditors also evaluate the following:

- Compliance with laws and regulations.
- Effectiveness of administrative controls and procedures.
- Efficiency of operations (also called operational auditing).
- Information to enable management to fulfilling its responsibilities under statutes, regulations, and directives such as those required by Sections 112 and 132 of Federal Deposit Insurance Corporation Improvement Act (FDICIA) and 12 CFR Part 363.
- Procedures to ascertaining the adequacy of controls to minimize risk of losses. One procedure is for internal auditors to appraise the soundness and adequacy of accounting, operating, and administrative controls. The appraisal process ensures that the association records transactions promptly and accurately, and properly safeguards assets.
- For example, a critical internal audit responsibility/procedure is to determine the adequacy of valuation allowances by reviewing the system and procedures for internal asset review and credit quality classifications.

## INDEPENDENCE OF INTERNAL AUDITORS

Internal auditors must maintain independence within the organization. The higher the level the auditor reports to within the organization, the greater the likelihood of achieving effective independence. The institution's policies should give the auditor the authority necessary to perform the job. That authority should include free access to any records necessary for the proper conduct of the audit.

Ideally, the internal auditor should report directly to an audit committee comprised of non-employee members of the board of directors. Reporting at this level should allow the auditor the greatest access to all levels of the institution, and assure prompt and independently objective consideration of audit results. It also enables the auditor to assist the directors in fulfilling their responsibilities.

The board of directors or its audit committee should regularly receive a report of all audit activity. This report should include the status of all audits on the internal audit schedule, and summaries of all audits completed during the period including audit conclusions. In addition, this report should provide the resolution status of previous internal audit findings and recommendations. If the internal auditor does not report to the board or its audit committee, the reporting line should be to an individual with no financial or operational responsibilities. Inadequate independence of internal auditors is cause for critical OTS examination report comments. Instances in which an internal auditor reports to management may warrant further consideration and assurance that independence of the internal auditor is not compromised.

Internal auditors' responsibilities and qualifications may vary, depending on the size of the institution and complexity of operations. The internal audit function is generally a full-time job of an individual or group, but may be a part-time job in smaller institutions. The institution may also outsource some or all of its internal audit work.

Large institutions often designate a chief auditor to supervise the work of an internal audit staff. In small institutions, the responsibility for internal audit may rest with officers or other employees designated as part-time auditors.

Small institutions with few employees and less complex operations may not have an internal auditor on staff. Nevertheless, the institution can ensure that it maintains an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls. The person given this task should not also be responsible for managing or operating those controls.

## INTERNAL AUDIT OUTSOURCING

Financial institutions are increasingly contracting with independent public accounting firms or other outside professionals to perform work traditionally conducted by internal auditors. These arrangements are frequently referred to as “internal audit outsourcing,” “internal audit assistance,” “audit integration,” “audit co-sourcing,” or “extended audit services.” Outsourcing arrangements create a variety of safety and soundness issues that will vary with the size, complexity, scope of activities, and risk profile of the bank and the nature of the outsourcing arrangement.

Financial institutions generally enter into internal audit outsourcing arrangements to gain operational or financial efficiencies by engaging a vendor to:

- Assist its internal audit staff when the bank’s internal auditors lack the expertise required for an assignment. Such assignments are most often in specialized areas such as information technology, fiduciary, mortgage banking, and capital markets activities. The vendor normally performs only certain agreed-upon-procedures in specific areas and reports findings directly to the institution’s internal audit manager.
- Perform the entire internal audit. The institution’s only internal audit staff may be an audit manager. The vendor usually assists the board and audit manager in determining the critical risks to be reviewed during the engagement, recommends and performs audit procedures approved by the internal auditor, and jointly with the internal auditor, reports significant findings to the board of directors or its audit committee.

In any outsourced arrangement, the institution should meet the following guidelines:

- An employee (generally an internal auditor or internal audit manager or director) who is independent and responsible should manage the relationship with the vendor.
- The directors have the responsibility for ensuring that any outsourcing arrangement is competently managed and that it does not detract from the scope or quality of an institution’s internal audit work, overall internal control structure of the institution, or audit and control evaluations.
- The board and management perform sufficient due diligence before entering into the outsourcing arrangement to verify the vendor’s competence and objectivity, and during the

arrangement to determine the adequacy of the vendor's work and compliance with contractual requirements.

- The arrangement does not compromise the role or independence of a vendor if the vendor also serves as the institution's external auditor.

If the institution outsources the internal audit function, or any portion of it, determine the effectiveness of and reliance to be placed on the outsourced internal auditing. You should obtain copies of the following documents:

- Outsourcing contracts or engagement letters.
- Outsourced internal audit reports and associated work papers.
- Policies on outsourced audit, if any.

Review the outsourcing contracts, engagement letters, work papers, and policies to determine whether they adequately do the following:

- Set the scope and frequency of work the outside vendor will perform.
  - Outsourced internal audit reports and internal audit work papers should be adequately prepared in accordance with the audit program and the outsourcing agreement.
  - Work papers should disclose the specific program steps, calculations, or other evidence that supports the procedures and conclusions set forth in the outsourced reports.
  - The scope of the outsourced internal audit procedures should be adequate regarding the procedures and testing performed, and the internal audit manager should approve the process.
  - The institution should revise the scope of outsourced audit work appropriately when the institution's environment, activities, risk exposures, or systems change significantly.
- Set the manner and frequency of reporting to the institution's audit manager, senior management, and audit committee or board of directors about the status of work.
  - The institution should subject the vendor to objective performance criteria such as whether an audit is completed on time and whether overall performance meets the objectives of the audit plan.
  - Key institution employees and the vendor should clearly understand the lines of communication and how the institution will address internal control or other problems noted by the vendor.

- Results of outsourced work should be well documented and reported promptly to the board of directors or its audit committee by the internal auditor, the vendor, or both jointly.
- Establish a process for changing terms of the service contract, especially for expansion of audit work if the auditor finds significant issues.
- State that internal audit reports are the property of the institution, that the vendor will provide copies of related work papers the institution deems necessary, and that authorized employees of the institution will have reasonable and timely access to work papers prepared by the outside vendor.
- Identify the locations of outsourced internal audit reports and related work papers.
- Grant OTS examiners immediate and full access to outsourced internal audit reports and related work papers.
- Prescribe an alternative dispute resolution process for determining who bears the cost of consequential damages arising from errors, omissions, and negligence.
- State that outside vendors, if subject to SEC or other independence guidance, such as that issued by the AICPA, will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee of the institution.
- Review the performance and contractual criteria for the vendors and any internal evaluations of the vendor, and determine if the board or audit committee performed sufficient due diligence to satisfy themselves of the vendor's competence before entering into an outsourcing arrangement.
- Determine if procedures exist to ensure that the vendor maintains sufficient expertise to perform effectively throughout the arrangement.
- Determine whether the vendors are independent, and disclose any potential conflicts of interest. If a vendor is an independent public accountant who also performs the institution's external audit, potential conflicts of interest may exist.
- The board should be familiar with AICPA Interpretation 102-2 about conflicts of interest under AICPA Rule 102, which discusses integrity and objectivity of independent public accountants performing outsourced internal audit work.

If you determine that you cannot rely on the vendor's work, discuss that assessment with the Regional Accountant, the board, bank management, and the affected party before finalizing the report of examination.

### Independence Issues and Outsourcing

The institution's board of directors, management, auditor, and OTS should pay particular attention to independence issues if both of the following occur:

- A savings association, holding company, or affiliate outsources internal audit work to its external auditor, and
- The internal audit work relates to internal accounting controls, financial systems, or financial statements.

Management should address independence issues and any other potential conflicts of interest that may arise when one firm performs both internal and external audit services.

The reason for the concern is that an auditor generally relies, at least to some extent, on the internal control system when performing the external audit. If the outside vendor that provides the internal audit services is also the external auditor, then the external auditor could be relying on his or her own work. Thus, the arrangement introduces significant questions about the independence of the external auditor, both in appearance and in fact. Such an arrangement may compromise the role or independence of a vendor. In cases where the same firm performs internal and external audit work, institutions may consider requesting that the audit firm use different accounting firm employees to perform the internal audit and external audit duties. (See Examiner Guidance in [Appendix A](#).)

OTS follows the Securities and Exchange Commission (SEC) regulations that impose substantial requirements and limitations on a savings association, a holding company, or an affiliate that outsource any internal audit work to its external auditor. OTS regulation 12 CFR Part 562.4 states that an independent public accountant must perform the external audit, whether required or otherwise, of a savings association, a holding company, or affiliate. Under this regulation, independent public accountants are subject to the independence requirements and interpretations of the SEC and its staff.

The SEC independence rules (17 CFR Parts 210 and 240) include substantial requirements and limitations with respect to providing any internal audit services to external audit clients. The effective date related to internal audit-related services is August 5, 2002.

Under the SEC independence rules, when the external auditor provides any internal audit services (including both (a) internal audit services related to internal accounting controls, financial systems, or financial statements, and (b) operational internal audit services) for an external audit client, the SEC requires management to do the following:

- Acknowledge in writing to the external auditor and the audit committee (or if there is no such committee, then the board of directors) management's responsibility to establish and maintain a system of internal accounting.
- Designate a competent employee or employees, preferably within senior management, to be responsible for the internal audit function.

- Determine the scope, risk, and frequency of internal audit activities, including those the external auditor will perform.
- Evaluate the findings and results arising from the internal audit activities, including those the external auditor performed.
- Evaluate the adequacy of the internal audit procedures performed, and the findings resulting from the performance of those procedures, by among other things, obtaining reports from the external auditor.
- Not rely on the external auditor's work as the primary basis for determining the adequacy of its internal controls.

In addition, where the external auditor provides internal audit services related to internal accounting controls, financial systems, or financial statements for an external audit client, the SEC limits these services to an amount not greater than 40 percent of the total hours expended on such internal audit activities in any one fiscal year. However, this limitation does not apply where the client company has less than \$200 million in total assets.

The AICPA also provides a list of activities that impair independence for its members. OTS considers the AICPA guidance on independence to be applicable to all independent public accountants performing external or internal audit work.

If you find sufficient reason to question a vendor's independence, objectivity, competence, or failure to meet OTS and SEC standards, discuss the situation with the Regional Accountant. If appropriate, request through the institution that the vendor make additional work papers available, and meet with the vendor to discuss concerns.

To provide uniform guidance on the internal audit function and outsourcing, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board, and the Office of Thrift Supervision issued the Interagency Policy Statement on the Internal Audit and Its Outsourcing on December 22, 1997. (Although the text of this handbook section incorporates the guidance, see [Appendix A](#) for the full text of the Interagency Policy Statement.)

## COMPETENCE OF INTERNAL AUDITORS

An audit manager, whether working alone or with staff, should possess the following qualifications:

- Academic or other credentials comparable with those of other institution officers with major responsibilities in the organization.
- Commitment to a program of continuing education and professional development.
- Audit experience, and organizational and technical skills commensurate with the responsibilities including proficiency in applying internal audit standards, procedures, and techniques.



- Strong oral and written communication skills.
- Ability to properly supervise each audit and provide suitable instructions to help meet audit objectives.

To understand fully the flow of data and the underlying operating procedures, the internal audit function manager must have proper education, training, and understanding of key areas of bank operations. College courses, various industry sponsored courses, and significant prior work experience in various departments of an institution may provide adequate education.

Certification as a certified internal auditor or a certified public accountant may serve as further evidence of having the appropriate credentials. The internal audit function manager must maintain a program of continuing education.

The audit staff should also possess certain minimum qualifications and skills commensurate with the complexity of the institution's operations. Any member of the audit staff in a supervisory position should possess adequate knowledge of audit objectives and an understanding of the audit procedures performed by the staff.

The final measures of internal auditors' competence and performance are the quality of the work performed, and the ability to communicate the results of that work. The adequacy of the audit program, the quality and completeness of internal audit work papers, and the clarity and comprehensiveness of internal audit reports reflect evidence of an auditor's competence and performance.

## THE AUDIT PLAN AND PROGRAMS

The overall audit plan, which consists of various departmental and functional audit programs, must attain the audit committee or the board of director's desired objectives. The audit committee or board should approve the audit plan at least annually. In assessing the adequacy of the annual audit plan and completed audit programs, evaluate the following areas:

- The audit plan's scope, frequency, and depth including any internal rating system as it relates to the institution's size, the nature and extent of its banking activities, and the institution's risk profile.
- Board of directors' or audit committee minutes, or summaries thereof. Determine whether the audit committee or board of directors formally approves the internal audit function's objectives, the audit program and schedule, and monitors the activities of the internal audit department to follow the approved programs and schedules. The audit committee or the board should approve any significant changes to the program or schedule.
- Management's records supporting any assertions concerning the effectiveness of internal controls over financial reporting and compliance with designated laws and regulations. Management should set its standards for measuring the adequacy and effectiveness of internal controls over financial reporting based on risk analyses or assessments, control assessments,

audit report findings, and other various resources including established standards such as those set by the AICPA.

- Content of the individual audit programs.
- Documentation of the work performed.
- Conclusions reached and reports issued.
- Procedures for follow-up to ensure the association take corrective action.

A characteristic of a good internal audit plan is a proactive approach. It should have an early warning system to detect and evaluate risks, determine scope, frequency, and depth of audit procedures needed, and adjust the audit plan accordingly.

In assessing risk, the auditor should consider the following factors:

- The nature and relative size of the specific operation and related assets and liabilities, including off-balance sheet transactions.
- The existence of appropriate policies and internal control standards.
- The effectiveness of operating procedures and internal controls.
- The potential materiality of errors or irregularities associated with the specific operation.

Audit programs are an integral part of the audit work papers, and serve as the primary evidence of the audit procedures performed. Before developing or revising the audit program, the internal auditor should have a thorough understanding of the operations of the department or function. The auditor should prepare or revise a written audit program for each area of an institution's operations before beginning the audit work.

Each program should contain a clear, concise description of the internal control objectives, degree of risk if internal controls fail, and the procedures to follow in testing such controls. An individual audit program may encompass several departments/functions of an institution, a single department, or specific operations within a department.

The effectiveness of the overall audit plan depends on a variety of factors. To plan effectively, the auditor must consider the factors described above, along with many of those outlined in [Examination Handbook Section 060, Examination Strategy, Scoping, and Management](#).

Most audit programs should address the following audit procedures:

- Surprise audits where appropriate.
- Maintenance of control over records selected for audit.

- Review and evaluation of the institution's policies and procedures and the system of internal controls.
- Reviews of laws, regulations, and rulings.
- Sample selection methods and results.
- Proof of reconciling detail to related control records.
- Verification of selected transactions and balances through examination of supporting documentation, direct confirmation and appropriate follow-up of exceptions, and physical inspection.

The internal audit work papers must document the work performed by the auditor. Work papers should contain completed audit work programs and analyses that clearly indicate the procedures performed, the extent of testing, and the basis for the conclusions reached.

Upon completion of the procedures outlined in audit programs, the internal auditor should be able to reach conclusions that will satisfy the audit objectives. The internal auditor must effectively interpret these conclusions documented in the work papers. Audit report findings must be consistent with the documented conclusions. Reports should include, when appropriate, recommendations for remedial action. The overall audit plan must also provide for follow-up procedures to ensure that the association takes corrective action.

The internal auditor must communicate all findings and recommendations in a clear, concise manner, pinpointing problems and suggesting solutions, and submit reports as soon as practicable. Auditors should route reports to those officials who have both the responsibility and authority to implement suggested changes. If full audit reports do not go to the board of directors, the auditor should prepare summary reports for the board's review. Prompt and effective management response to the auditor's recommendations is the final measure of the effectiveness of the audit program. The auditor should inform the audit committee or board of management's responses to audit findings and recommendations.

### Information Systems and Technology Audit Review

The institution's internal audit program should have qualified personnel review, test, and evaluate the information systems and technology environment. The Federal Financial Institutions Examination Counsel (FFIEC) Information Technology Handbook contains examination policies and procedures that govern the assessment of the information systems and technology audit function by all financial institution regulators.

The internal audit program should provide audit coverage of significant information systems and technology risk exposures. This would include systems development projects and computer production activities involving on-premise computing (for example, on stand-alone and networked microcomputers), in-house computer centers, and third-party vendors (for example, service bureaus).

The scope of the internal audit program should also address information system and technology-related threats from outside sources (for example, unauthorized access to the institution's or their service provider's on-line banking operation).

## FEDERAL DEPOSIT INSURANCE CORPORATION IMPROVEMENT ACT (FDICIA) – SECTION 112

In May 1993, the Board of the FDIC approved the initial regulations and guidelines implementing the management reporting, audit committee, and annual independent audit requirements of § 112 of FDICIA. Congress amended the statute by passing the Economic Growth and Regulatory Paperwork Reduction Act (EGRPRA) of 1996. The regulations apply to insured depository institutions with total assets of \$500 million or more. The requirements for these institutions include the following:

- Reporting to the FDIC and OTS (when it is the primary regulator) on internal control over financial reporting and compliance with certain laws and regulations, as well as filing annual audited statements.
- An annual audit by an independent public accountant (external auditor).
- An audit committee consisting of outside directors, who must be independent of management. For institutions holding over \$3 billion in assets, two of the outside directors must have banking and financial management expertise, neither can be a large customer of the institution, and they must have independent access to the audit committee's outside counsel.

### Management Assertions

To assist management in determining strategies related to management's reporting on both the effectiveness of internal control over financial reporting and compliance with designated laws such as FDICIA and regulations, the internal auditor may:

- Test the effect of key controls identified as a basis for management's assertions.
- Perform agreed-upon procedures to test compliance with laws and regulations.
- Establish a system to monitor the internal control system and identify changes needed in the control environment.

Management may use the internal auditor's work to facilitate its assertion that the internal control over financial reporting is effective. The internal auditor's procedures must be sufficient for management to rely on them for such assertions.

The external auditor performs examination procedures to attest to management's assertion that the internal control over financial reporting is functioning effectively. The external auditor may consider the work done by the internal auditor as part of the auditing procedures.

## REGULATORY CONCERNS

Your review and evaluation of the internal audit function is key in determining the scope of the examination. You should separately determine the adequacy and effectiveness of the audit program for each area of examination interest.

The internal auditor's work may provide useful information in setting the scope of the examination. You should judge the independence and competence of the internal auditor before addressing the overall adequacy and effectiveness of audit programs, and the work performed. If, for example, you conclude that the internal auditor possesses neither the appropriate independence nor the competence, you cannot rely upon the work for scoping purposes.

To test the adequacy of the internal audit work, follow the Internal Audit Program Level I and II procedures. Level I procedures describe the use of the Internal Audit Questionnaire.

Under Level II procedures, you may review work papers that document and test procedures performed by internal auditors. In some cases, such a review may be sufficient to substantiate conclusions about the quality and reliability of the internal audit function. The Internal Auditor Questionnaire from the PERK package should provide pertinent information. [See Appendix B](#). Findings from the internal audit work paper reviews will also help you determine whether further verification procedures and testing are necessary under Level III procedures.

After reviewing work papers and testing procedures, report the following weaknesses in internal audit-related management and internal controls to the Regional Accountant:

- Absence of or inadequacy of an internal audit function in a large institution or an institution with complex operations.
- An inadequate internal audit plan.
- Instances in which the internal auditor does not have full access to records or otherwise lacks independence.
- Lack of internal auditor competence and/or expertise.
- Instances in which the internal auditor reports to operational officers rather than the board of directors or audit committee of outside directors.
- Audit committees not properly established or non-functioning, such that they are unable to initiate corrective action.

## Other Internal Audit Resources

The institution may also provide you with a Global Audit Information Network (GAIN) report purchased from the Institute of Internal Auditors or a similar product by another vendor. Generally

these products are Internet-based and may provide information about general organization statistics, audit staff profiles, quality assurance practices, audit committee information, scope of internal audit activities, audit planning, risk assessments, and other audit information you may find useful. OTS does not endorse these products or require institutions to use them, but if such information is available, consider requesting it to review for scoping your examination.

## REFERENCES

### Code of Federal Regulations (12 CFR)

Part 562                      Regulatory Reporting Standards

### Internal Audit Guidance

\*The Institute of Internal Auditors' Standards for the Professional Practice of Internal Auditing

\*Financial Managers Society's Financial Institutions Internal Audit Manual, 2000-200

Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees (1999)

\* Internal audit staff may have these documents in-house.

### American Institute of Certified Public Accountants

#### *Statements on Auditing Standards (U.S. Auditing Standards (AU))*

- |        |   |
|--------|---|
| No. 41 | Working Papers, Providing Access to or Photocopies of Working Papers to a Regulator, AU 339)      |
| No. 55 | Consideration of the Internal Control Structure in a Financial Statement Audit (AU 319)           |
| No. 58 | Reports on Audited Financial Statements (AU 508)  |
| No. 60 | Communication of Internal Control Structure Related Matters Noted in an Audit (AU 325 and 9325)   |
| No. 61 | Communication with Audit Committees (AU 380)  |
| No. 78 | Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55 (AU 319) |
| No. 82 | Consideration of Fraud in a Financial Statement Audit (AU 316)                                    |
| No. 89 | Audit Adjustments (AU 420)  |

- No. 90                      *Audit Committee Communications (AU 380)*
- No. 94                      *The Effect of Information Technology on the Auditor's Consideration of  
Internal Control in a Financial Statement Audit (AU 319)*

**This page intentionally left blank**



# Internal Audit Program

---

## EXAMINATION OBJECTIVES

To determine whether the internal audit function is consistent with the institution's size, complexity of operations, level of growth, investment and operations risk profile, nature and severity of previous examination findings.

To evaluate the independence, expertise, and competence of internal auditing staff.

To determine the adequacy of the procedures performed by the internal auditors.

To evaluate the internal auditor's identification of areas of risk within the institution and structuring of the overall audit approach to cover these areas of risk.

To determine whether the internal auditor's work and reports are reliable.

To determine if the internal auditor has an effective system for following up on problems and recommendations, and if the institution has taken corrective action for deficiencies noted by the internal auditor.

To determine the overall effectiveness of the internal audit function in strengthening internal controls and in monitoring adherence to controls, procedures, and regulatory requirements by management and employees.

## EXAMINATION PROCEDURES

### LEVEL I

WKP. REF.

1. Evaluate the scope of the internal audit work based on the answers to the Internal Auditor Questionnaire, review the internal audit plan, including adjustments to the plan based on any early warning system that detects risks, any prior internal audit report ratings, and the results of previous reviews of the auditor's work. Review minutes of the audit committee. Discuss with regulatory staff assigned the review of the board minutes, possible areas of concern that the internal audit staff should have addressed.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Audit Program

---

WKP. REF.

2. Interview the internal audit staff and observe the operation of the audit function to determine its organizational responsibilities. Be alert to any information indicating lack of independence of the internal audit staff, including whether management places any restrictions on the audit programs or imposes any unreasonable scheduling or budgetary restraints. Determine whether the auditor maintains independence in appearance, and approaches the audit process in an ethical and professional manner.  

---
3. If the institution outsources its internal audit function, review the contract to ensure the arrangement is consistent with interagency guidelines. (Appendix A, Interagency Policy Statement on the Internal Audit Function and its Outsourcing; and Sections 310 and 340.) Consult with the regional accountant for additional guidance.  

---
4. Review the internal audit department for the existence of any operational duties regarding auditors, any family ties with non-audit employees, or any other relationships incompatible with maintaining an independent internal audit function.  

---
5. Review the audit plan for completeness and for evidence of compliance with proper board or audit committee approval procedures. Ensure the audit committee or the board performs periodic assessments of the internal audit function and takes appropriate action to ensure ongoing reliability and effectiveness.  

---
6. Review the organization chart and the institution's chart of accounts. Note whether the internal auditor considers all existing service corporations, subsidiaries, joint ventures, and significant accounts. Ensure that the internal auditor performed an assessment of risk for each audit area.  

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Audit Program

---

WKP. REF.

7. During the initial review of the internal audit function, review audit manual(s) and associated material to determine whether prescribed procedures are sufficient for accomplishing the audit objectives.  

---
8. Determine whether the institution modifies internal audit programs in a timely manner to keep pace with changes in institution activities, economic environment, technology, and regulations.  

---
9. Review audit reports by internal auditors and determine whether management provided satisfactory responses and adopted any recommended changes. Determine the reason for any recommendations not addressed by management.  

---
10. Review Level II procedures and perform those necessary to test, support, and present conclusions derived from performance of Level I procedures.  

---

## LEVEL II

1. Determine if the institution has recently changed internal auditing personnel. If so, discuss the reasons for such change with management. Pay particular attention to any disagreements between the prior auditor and the institution regarding matters of accounting principles or practices, financial statement disclosures, internal controls, or auditing procedures and findings. Determine the validity of reasons given for any such changes. Consider contacting an auditor who the association terminated or who resigned.  

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Audit Program

---

WKP. REF.

2. Review a representative sample of audit reports and associated work papers to determine that they are adequate, prepared in accordance with the audit program, in compliance with prescribed procedures, and properly documented. Determine that the auditor tests the reliability of information produced in the institution. Determine who gets the reports. Answer the questions on the Internal Auditor Questionnaire to assist in your review of the audit program.  

---
3. Check for progress in correcting any earlier reported areas with significant weakness. Identify the responsible party to make the correction and the time frame.  

---
4. Check the adequacy of information on the audit function available to management and the board of directors or its audit committee.  

---
5. Ensure that your review meets the Objectives of this Handbook Section. State your findings and conclusions, and appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.  

---

## LEVEL III

Consider Level III procedures if after completing both Level I and II procedures you are unable to make firm assessments of the effectiveness of the institution's internal audit function. Be sure to apprise the EIC or FM of the need to perform Level III procedures.

1. If concerns about the auditor's work exist, check the accuracy of selected audit findings by duplicating the procedures of the auditor. For example, on a test basis, review loan files that the auditor reviewed, following the same procedures. If findings differ significantly, review your findings with management and/or the audit

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Internal Audit Program

---

WKP. REF.

committee. Test for evidence of insider abuse, known or suspected defalcations, known or suspected criminal activity, and questionable transactions with affiliates.

---

2. Determine if the internal audit department's role in automated or manual systems design is adequate. Review uses of the computer and determine if internal audit staff have access to the files for audit purposes.
- 

3. For internal audit personnel hired since the last examination (or for the entire audit staff if not previously examined), review personnel files for information such as: level of education attained, significant work experience, certification as an internal auditor or a public accountant, and membership in professional associations. In a large internal audit department, the initial review should include the department manager and a sample of audit supervisors and staff. Consider adequacy of internal audit staff's qualifications, experience, and knowledge of key areas of operation, particularly if the institution has changed its primary business line or type of lending.
- 

## EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

**This page intentionally left blank**

---

# Internal Audit

## Questionnaire

---

Yes No

---

### GENERAL QUESTIONNAIRE

Review reports and the appropriate programs and work papers of the auditors in order to answer the following audit function questions. Where appropriate, retain supporting documentation and pertinent information or note it under "Comments."

*Explain all "No" answers.*

- |    |  |                          |                          |
|----|--|--------------------------|--------------------------|
| 1. | Has the auditor devised an overall audit plan identifying areas of risk?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. | Do programs and questionnaires exist for each area?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. | Is the independence of the internal auditor assured, based upon review of documentation such as the function's charter or the organization chart of the institution?             | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. | If the institution outsources responsibility for the internal audit function, does the outside contractor remain independent and not act in a capacity equivalent to management? | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Does the arrangement comply with current AICPA guidance?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. | Where the auditor used operating personnel, is there documentation showing that:   |                          |                          |
|    | • Either the auditor, or someone the auditor directs, closely supervised the operating personnel's work?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • They did not audit records of the department to which they are assigned or their own work?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. | Does the internal auditor meet with the directors at least annually to discuss written reports of audit?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • How often? _____   |                          |                          |
| 7. | Do audit programs include tests of physical and accounting controls performed in the following (minimum) areas:  |                          |                          |
|    | • Cash?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Consigned items and other nonledger control accounts?  | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Investments?   | <input type="checkbox"/> | <input type="checkbox"/> |
|    | • Loans?   | <input type="checkbox"/> | <input type="checkbox"/> |

**Exam Date:** \_\_\_\_\_

**Prepared By:** \_\_\_\_\_

**Reviewed By:** \_\_\_\_\_

**Docket #:** \_\_\_\_\_

---

## Internal Audit

## Questionnaire

---

	Yes	No
• Loans and participations sold and purchased?	<input type="checkbox"/>	<input type="checkbox"/>
• Allowances for credit losses?	<input type="checkbox"/>	<input type="checkbox"/>
• Deposits?	<input type="checkbox"/>	<input type="checkbox"/>
• Confirmation of loans and deposits?	<input type="checkbox"/>	<input type="checkbox"/>

Note: Detailed questions concerning the internal audit staff work in each of these areas follow.

### Cash

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal audit staff count and balance cash on hand?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • How often? _____  |                          |                          |
| • Do they make cash counts on a surprise basis?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Do they test bank account reconciliations for accuracy?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Do they test cash receipt procedures?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Do they test cash disbursement procedures?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Do they review cash control records and trace any apparently large or unusual cash movements to or from a department or branch? | <input type="checkbox"/> | <input type="checkbox"/> |

### Funds Transfer Activities

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor review the wire transfer function for segregation of duties involving receipt, processing, settlement, accounting, and reconciliation? | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor test staff compliance with credit and personnel procedures, operating instructions, and internal controls?                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor review overnight drafts?   | <input type="checkbox"/> | <input type="checkbox"/> |

### Due From Banks

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor test the bank reconciliation including the Federal Reserve Bank?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Do they receive cut-off bank statements as of the examination date and an appropriate date subsequent to the examination date for use in testing bank reconciliation? | <input type="checkbox"/> | <input type="checkbox"/> |

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



---

## Internal Audit

### Questionnaire

---

- |  | Yes                      | No                       |
|--|--------------------------|--------------------------|
| 2. Does the internal auditor review all returned items for an appropriate period subsequent to the examination date?                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor confirm due from banks?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor check the accuracy and completeness of reports submitted to the Federal Reserve for calculation of required reserve balances? | <input type="checkbox"/> | <input type="checkbox"/> |

#### Consigned Items and Other Nonledger Control Accounts

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 1. Does the internal auditor balance and confirm consignment items?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • How often? _____   |                          |                          |
| • On a surprise basis?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor test income from the sale of consignment items?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor test rental income for safe deposit boxes?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor check vault entry records for signature(s) of authorized persons?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Does the internal auditor examine safekeeping/custodial accounts or confirm them with an outside custodian?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Does the internal auditor test the completeness of safekeeping/custodial items and records by examining supporting documentation or by confirming with customers?                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Does the internal auditor test closed safekeeping/custodial accounts?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 8. Does the internal auditor test fee income for safekeeping/custodial accounts?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 9. Does the internal auditor test collection items by examining supporting documentation, subsequent receipt of payments, disbursement to customers of funds collected, or by confirming with customers? | <input type="checkbox"/> | <input type="checkbox"/> |
| • Does the internal auditor test collection fee income?  | <input type="checkbox"/> | <input type="checkbox"/> |

#### Investments

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 1. Does the internal auditor verify that the board adopted written investment policies that include the institution's investment limits, each trader's limits, etc.? | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor examine or confirm all investment securities?   | <input type="checkbox"/> | <input type="checkbox"/> |

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

	Yes	No
3. Has the internal auditor ascertained that securities transactions are in keeping with stated portfolio objectives?	<input type="checkbox"/>	<input type="checkbox"/>
Has the internal auditor also:		
• Reviewed the securities dealers with who the institution conducts securities activities?	<input type="checkbox"/>	<input type="checkbox"/>
• Reviewed objectionable investment portfolio transactions?	<input type="checkbox"/>	<input type="checkbox"/>
4. Does the internal auditor test that all investment securities transactions are authorized?	<input type="checkbox"/>	<input type="checkbox"/>
5. Does the internal auditor verify investment securities balances (including physical count of securities located in the institution, and confirm institution ownership and control of securities held in custody outside the institution)?	<input type="checkbox"/>	<input type="checkbox"/>
6. Does the internal auditor verify the book and market values of investment securities?	<input type="checkbox"/>	<input type="checkbox"/>
7. Does the internal auditor reconcile the accrued interest accounts to detail, and check computations of interest income?	<input type="checkbox"/>	<input type="checkbox"/>
8. Does the internal auditor test the gain and loss on investment securities sold during the period?	<input type="checkbox"/>	<input type="checkbox"/>
9. Does the internal auditor review hedging activities (forward commitments, futures, options, and interest rate swaps) for compliance with internal policies and procedures and strategies?	<input type="checkbox"/>	<input type="checkbox"/>
10. Does the internal auditor check for compliance with laws and regulations applicable to those savings institutions engaging in the purchase or sale of securities instruments for their own account or for the account of customers (including providing commodity advice to customers)?	<input type="checkbox"/>	<input type="checkbox"/>
11. Does the internal auditor check for compliance with the FFIEC "Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities?"	<input type="checkbox"/>	<input type="checkbox"/>
12. Does the internal auditor check for compliance with the repurchase agreement provision of the Government Securities Act for non-dealer entities?	<input type="checkbox"/>	<input type="checkbox"/>

#### Retail Nondeposit Investment Sales

1. Does the internal auditor check the monitoring and resolution of customer complaints?	<input type="checkbox"/>	<input type="checkbox"/>
2. Does the internal auditor test customer accounts for proper disclosures?	<input type="checkbox"/>	<input type="checkbox"/>

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

- |   | Yes                      | No                       |
|---|--------------------------|--------------------------|
| 3. Does the internal auditor check for conflicts of interest?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor review the saving association's compensation program for retail nondeposit investment product sales?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. If the savings association has a separate compliance program for retail nondeposit investment product sales, did the internal auditor review the adequacy of the compliance program?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Where the savings association offers retail nondeposit investment products through an independent third-party vendor, did the internal auditor review vendor adherence to the governing agreement?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Did the internal auditor ascertain that the sales activities were in keeping with established policies and procedures, applicable laws, and regulations, and the February 15, 1994, "Interagency Statement on Retail Sales of Nondeposit Investment Products?" | <input type="checkbox"/> | <input type="checkbox"/> |

#### Subordinate Organizations and Affiliates

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor review and test the investment in and the transactions with related organizations?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor determine that investments, advances, or transactions with affiliates are consistent with covenants of debt or other instruments as approved by the board of directors or bank management? | <input type="checkbox"/> | <input type="checkbox"/> |

#### Derivatives

The level of internal auditor expertise should be consistent with the level of activity and degree of risk assumed by the savings association. In some cases, a savings association may need to outsource internal audit coverage of derivative activities to ensure that the persons performing the audit work possess sufficient depth and experience.

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor assess the adequacy and reasonableness of information obtained and used in risk management systems (market, credit, liquidity, and operation and systems)? | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor validate the data integrity of significant market, liquidity, and risk management models?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the external auditor determine that contract documentation is properly maintained and safeguarded, and ascertain that legal counsel has properly reviewed documents?            | <input type="checkbox"/> | <input type="checkbox"/> |

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

- |  | Yes                      | No                       |
|--|--------------------------|--------------------------|
| 4. Has the external auditor confirmed the effectiveness of internal control systems used for derivatives transaction processing and valuation?                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Has the external auditor checked compliance with laws, rules, regulation, proper accounting, and taxation considerations?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Has the internal auditor ascertained the savings association staff performs derivative activities within the guidelines provided by bank policies and procedures? | <input type="checkbox"/> | <input type="checkbox"/> |

#### Loans

(Loans include commercial loans, installment loans, floor plan loans, credit card loans, home equity, and construction).

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor determine if the institution maintains up-to-date documentation showing lending policies and procedures?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor determine whether compliance with policies and procedures is adequate?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor test delinquency lists?<br>• How often? _____  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor test interest and accrual computations?<br>• How often? _____  | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Does the internal auditor verify loan and escrow (impound) account balances (including confirmation procedures)?<br>• Does the internal auditor physically inspect collateral, if applicable?<br>• Has the internal auditor tested the pricing of negotiable collateral, if applicable?                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 6. Does the internal auditor examine notes and other legal documentation for authorized approvals and compliance with policies?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 7. Do the internal auditor's work papers disclose:<br>• The number and percent of new loan files examined compared with the total originated during the period?<br>• The number and percent of files applicable to previous audit periods examined compared with the total number outstanding as of the audit date? | <input type="checkbox"/> | <input type="checkbox"/> |

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

	Yes	No
<ul style="list-style-type: none"><li>• The basis used for selection of loan accounts for inspection and the specific documents inspected?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
8. Does the internal auditor note all material exceptions?	<input type="checkbox"/>	<input type="checkbox"/>
9. Does the internal auditor determine the adequacy of insurance coverage and ensure that the institution names itself as loss payee?	<input type="checkbox"/>	<input type="checkbox"/>
10. Does the internal auditor verify the loan-in-process accounts?	<input type="checkbox"/>	<input type="checkbox"/>
11. Does the internal auditor review the sales of repossessed collateral/foreclosed mortgages to determine the propriety of the entries made to record the sales?	<input type="checkbox"/>	<input type="checkbox"/>

#### Loans and Participations Sold or Purchased

1. Do the internal auditor's work papers indicate the extent of audit procedures performed and conclusions reached?	<input type="checkbox"/>	<input type="checkbox"/>
2. Does the internal auditor confirm: <ul style="list-style-type: none"><li>• Significant balances of loans and participations sold or purchased?</li><li>• Significant terms of purchase or sales agreements?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
3. Do the internal auditor's work papers indicate the methods used to determine the adequacy of auditing procedures on loans serviced by others?	<input type="checkbox"/>	<input type="checkbox"/>
4. Do the internal auditor's procedures include, when appropriate, obtaining letters from servicing organizations' auditors confirming the extent of their audit procedures?	<input type="checkbox"/>	<input type="checkbox"/>
5. For loans purchased, do the internal auditor's procedures verify that: <ul style="list-style-type: none"><li>• The underwriting meets the institution's underwriting standards?</li><li>• The institution obtains, reviews, and retains all pertinent documents?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>

#### Mortgage Banking Activities

1. Does the internal auditor test book and fair-market values of mortgage servicing assets?	<input type="checkbox"/>	<input type="checkbox"/>
2. Does the internal auditor verify the appropriateness of hedge accounting?	<input type="checkbox"/>	<input type="checkbox"/>
3. Does the internal auditor test the accuracy of tracking systems by verifying that documentation was on hand, or in process of being received, for loans awaiting sales and those being serviced?	<input type="checkbox"/>	<input type="checkbox"/>

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

	Yes	No
<ul style="list-style-type: none"><li>• Did the internal auditor follow up on any exceptions outstanding over 120 days?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
4. Does the internal auditor test impairment analyses?	<input type="checkbox"/>	<input type="checkbox"/>
5. Does the internal auditor determine the accuracy of financial reporting systems and other management information systems?	<input type="checkbox"/>	<input type="checkbox"/>
6. Does the internal auditor check compliance with established policies and procedures, accounting procedures, laws, rules, and regulations?	<input type="checkbox"/>	<input type="checkbox"/>

#### *Leasing Activities*

1. Does the internal auditor confirm leases and related balance sheet accounts?	<input type="checkbox"/>	<input type="checkbox"/>
2. Does the internal auditor review the leases and other legal documentation?	<input type="checkbox"/>	<input type="checkbox"/>
3. Does the internal auditor test the computation of depreciation expense, interest expense, or rental income?	<input type="checkbox"/>	<input type="checkbox"/>
4. Does the internal auditor test the computation of any gain or loss on sales and disposals of property and trace the sales proceeds to cash receipts records?	<input type="checkbox"/>	<input type="checkbox"/>
5. Does the internal auditor determine that account balances accurately reflect any deferred tax liability or asset?	<input type="checkbox"/>	<input type="checkbox"/>
6. Does the internal auditor review insurance coverage and determine that property damage coverage is adequate in relation to book value and that liability insurance is in effect?	<input type="checkbox"/>	<input type="checkbox"/>

#### Allowances for Credit Losses

1. In determining the adequacy of the general and specific allowances for credit losses, including the allowance for loan and lease losses (ALLL):		
<ul style="list-style-type: none"><li>• Does the internal auditor verify loan balances for the loans charged off since the last audit?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"><li>• Does the internal auditor examine the supporting documentation for loans charged off?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"><li>• Does the internal auditor reconcile loan recovery detail amounts to credit entries in the appropriate general ledger accounts?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>
<ul style="list-style-type: none"><li>• Does the internal auditor assess whether the ALLL is adequate to provide for losses for the remaining life of all classified loans and for the next 12 months for the loans that are not classified?</li></ul>	<input type="checkbox"/>	<input type="checkbox"/>

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

- |  | Yes                      | No                       |
|--|--------------------------|--------------------------|
| 2. Does the internal auditor verify that the institution uses a board-approved method to determine the need for and adequacy of allowances for credit losses?                                | <input type="checkbox"/> | <input type="checkbox"/> |
| • Does this methodology comply with OTS policy, GAAP, and industry practice?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Is an adequate record available indicating which assets the internal auditor reviewed for classification and when?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor consider self-classifications of loans in determining the adequacy of the allowances for credit losses?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5. Does the internal auditor test the recording of deferred tax credits (charges) if the deduction for loan losses on the thrift's tax return was different from that charged to operations? | <input type="checkbox"/> | <input type="checkbox"/> |

#### Deposits: Demand, Time Deposit Savings Accounts, and other Transaction Accounts

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 1. Does the auditor maintain up-to-date documentation showing savings policies and practices?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Is the extent of the internal auditor's tests to determine compliance with board-approved policies and practices adequate?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor address the following (minimum) areas for dual control and segregation of duties:   |                          |                          |
| • Inactive accounts?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Closed accounts: Does the internal auditor test closed accounts and determine that they were properly closed?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Dormant accounts: Does the internal auditor test account activity in dormant accounts, bank-controlled accounts, employee/officer accounts, and accounts of employees'/officers' business interests? | <input type="checkbox"/> | <input type="checkbox"/> |
| • Passbooks and certificates?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Certificates of deposit: Does the internal auditor account for numerical sequence of pre-numbered certificates of deposits?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Opening accounts?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Closing accounts?  | <input type="checkbox"/> | <input type="checkbox"/> |

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

## Internal Audit Questionnaire

	Yes	No
• Loans on deposits?	<input type="checkbox"/>	<input type="checkbox"/>
• Account transfers?	<input type="checkbox"/>	<input type="checkbox"/>
• Interest (dividend) computation?	<input type="checkbox"/>	<input type="checkbox"/>

### Confirmation of Loans, Demand, Time Deposit Savings Accounts, and Other Transaction Accounts

1. Does the internal auditor use an adequate method to determine the extent of confirmation?	<input type="checkbox"/>	<input type="checkbox"/>
2. Do the internal auditor's work papers show the number and percent (both by number and dollar amount) of loans and deposit accounts confirmed?	<input type="checkbox"/>	<input type="checkbox"/>
• What basis does the internal auditor use to select accounts to confirm? _____		
• Is it appropriate?	<input type="checkbox"/>	<input type="checkbox"/>
3. If the internal auditor uses statistical sampling, do the work papers disclose:		
• The method used?	<input type="checkbox"/>	<input type="checkbox"/>
• A selection system with a random start?	<input type="checkbox"/>	<input type="checkbox"/>
• The confidence level achieved?	<input type="checkbox"/>	<input type="checkbox"/>
4. Does the internal auditor report all material exceptions?	<input type="checkbox"/>	<input type="checkbox"/>
5. Does the internal auditor review overdraft accounts and determine collection potential?	<input type="checkbox"/>	<input type="checkbox"/>

### OFFICIAL CHECKS

1. Does the internal auditor reconcile account balances?	<input type="checkbox"/>	<input type="checkbox"/>
2. Does the internal auditor determine the validity and completeness of outstanding checks?	<input type="checkbox"/>	<input type="checkbox"/>
3. Does the internal auditor examine documentation supporting paid checks?	<input type="checkbox"/>	<input type="checkbox"/>
4. Does the internal auditor test certified checks to customers' collected funds balances?	<input type="checkbox"/>	<input type="checkbox"/>

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



---

## Internal Audit

### Questionnaire

---

Yes    No

---

#### Other

1. Does the internal auditor test borrowings for approval and regulatory compliance?  Yes  No
- How often? \_\_\_\_\_
  - Does the internal auditor confirm borrowed funds?  Yes  No
  - Does the internal auditor examine supporting legal documents, disclosures, and collateral custody agreements, and determine compliance with applicable laws and regulations?  Yes  No
  - Does the internal auditor review the minutes of the stockholders' and board of directors' meetings for approval of all borrowing requiring such approval?  Yes  No
  - Does the internal auditor verify changes in capital notes outstanding?  Yes  No
  - Does the internal auditor review the accrued interest accounts and test computation of interest expense?  Yes  No
2. Does the internal auditor review the adequacy of the scope of auditing procedures for Other Liabilities and Deferred Credits?  Yes  No
- Does the internal auditor confirm balances of "other liability" accounts (including tests for unrecorded liabilities as of a given date)?  Yes  No
  - Does the internal auditor review the operation and use of any "inter-office" account?  Yes  No
  - Does the internal auditor review suspense accounts to determine that appropriate staff clears all items on a timely basis?  Yes  No
3. Does the internal auditor review whether the scope for auditing real estate owned (REO) accounts is adequate?  Yes  No
- Does the internal auditor review procedures to ensure that the institution purchases appropriate hazard insurance?  Yes  No
  - Does the internal auditor review current appraisal procedures, market values, and sales prices?  Yes  No
  - Does the internal auditor review foreclosure procedures including whether the institution has proper title?  Yes  No

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

### Questionnaire

---

- |  | Yes                      | No                       |
|--|--------------------------|--------------------------|
| • Does the internal auditor verify expenses to maintain properties, and confirm rental income?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Does the internal auditor review monthly reconciliations of the properties to the general ledger?  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Does the internal auditor review REO reports to the board of directors?  | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor's scope for auditing fixed assets include the following procedures:   |                          |                          |
| • Examining support for additions, sales, and disposals?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Reviewing property transactions with "bank-affiliated personnel?"  | <input type="checkbox"/> | <input type="checkbox"/> |
| • Verifying property balances?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Testing computation of depreciation expense?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Testing computation of gain or loss on property sales and disposals and tracing sales proceeds to cash receipts records?   | <input type="checkbox"/> | <input type="checkbox"/> |
| • Determining that any deferred tax liability or asset, evolving from the use of different depreciation methods for book and tax purposes is properly reflected on the bank's books? | <input type="checkbox"/> | <input type="checkbox"/> |

#### Accounts Receivable

1. Does the internal auditor perform any of the following procedures:
  - Confirm loan balances?
  - Review, or confirm with outside custodian, notes and other legal documentation including collateral?
  - Review the accrued interest accounts and check computation of interest income?

#### Other Assets

1. Does the internal auditor perform any of the following procedures:
  - Confirm balances and examine support for additions and disposals?

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

## Questionnaire

---

Yes    No

---

### Income and Expense

1. Does the internal auditor's scope adequately address all significant income and expense accounts?  Yes  No
- Does the internal auditor test income and expenses by examining supporting documentation for authenticity and proper approval?  Yes  No
  - Does the internal auditor test accruals by either recomputing amounts or examining documents supporting such accruals?  Yes  No
  - Test computations for gains and losses on disposals, and for amortizations?  Yes  No
  - Review inter-office transactions and suspense accounts to determine whether all items included were temporary?  Yes  No

### Capital Stock

1. If an institution acts as its own transfer agent and/or registrar, does the internal auditor account for all stock certificates (issued and unissued) and reconcile par value of outstanding shares to appropriate general ledger control accounts?  Yes  No
2. If an institution has an outside transfer agent and/or registrar, did the internal auditor confirm activity and verify that shares were issued since the previous audit?  Yes  No
3. Does the internal auditor review capital changes?  Yes  No

### Dividends

1. Does the internal auditor verify computation of dividends paid and/or accrued on stock?  Yes  No
2. Does the internal auditor review the minutes of the board of directors' meetings to verify the propriety and accrual of the dividend payment?  Yes  No

### Information System Services

1. Does the internal auditor perform periodic audit procedures for significant automated applications to determine that workflow is processed accurately and is in conformity with operating manuals?  Yes  No
2. Does the internal auditor control or periodically review dormant accounts?  Yes  No
3. Does the internal auditor review unposted items?  Yes  No

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

## Internal Audit

## Questionnaire

---

Yes    No

---

### Payment System Risk

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor test the bank's self-assessment?                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor review the reasonableness of any de minimis cap?   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor ascertain compliance with established bank policy? | <input type="checkbox"/> | <input type="checkbox"/> |

### Asset Management

- |   |                          |                          |
|---|--------------------------|--------------------------|
| 1. Does the internal auditor test fee income and client reimbursement?                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 2. Does the internal auditor examine asset management client contracts?                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3. Does the internal auditor check for compliance with applicable laws, regulations, and rulings? | <input type="checkbox"/> | <input type="checkbox"/> |
| 4. Does the internal auditor ascertain adherence with established bank policies and procedures?   | <input type="checkbox"/> | <input type="checkbox"/> |

### Branches

- |  |                          |                          |
|--|--------------------------|--------------------------|
| 1. Has the internal auditor performed appropriate audit procedures in the branches during a reasonable audit cycle that are at least as comprehensive as those listed in the applicable areas above? | <input type="checkbox"/> | <input type="checkbox"/> |
|--|--------------------------|--------------------------|

### COMMENTS

---

---

---

---

---

---

---

---

---

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

---

**BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM  
FEDERAL DEPOSIT INSURANCE CORPORATION  
OFFICE OF THE COMPTROLLER OF THE CURRENCY  
OFFICE OF THRIFT SUPERVISION**

**INTERAGENCY POLICY STATEMENT ON THE  
INTERNAL AUDIT FUNCTION AND ITS OUTSOURCING**

**December 22, 1997**

## INTRODUCTION

Effective internal control<sup>1</sup> is a foundation for the safe and sound operation of a banking institution or savings association (hereafter referred to as institution). The board of directors and senior managers of an institution are responsible for ensuring that the system of internal control operates effectively. Their responsibility cannot be delegated to others within the institution or to outside parties. An important element of an effective internal control system is an internal audit function. When properly structured and conducted, internal audit provides directors and senior management with vital information about weaknesses in the system of internal control so that management can take prompt, remedial action. The agencies' long-standing examination policies call for examiners to review an institution's internal audit function and recommend improvements if needed. In addition, more recently, the agencies adopted Interagency Guidelines Establishing Standards for Safety and Soundness, pursuant to Section 39 of the Federal Deposit Insurance Act (FDI Act).<sup>2</sup> Under these guidelines, each institution should have an internal audit function that is appropriate to its size and the nature and scope of its activities.

In addressing various quality and resource issues, many institutions have been engaging independent public accounting firms and other outside professionals (hereafter referred to as outsourcing vendors) to perform work that has been traditionally done by internal auditors. These arrangements are often called "internal audit outsourcing," "internal audit assistance," "audit co-sourcing," and "extended audit services" (hereafter, collectively referred to as outsourcing).

Such outsourcing may be beneficial to an institution if it is properly structured, carefully conducted, and prudently managed. However, the federal banking agencies have concerns that the structure, scope, and management of some internal audit outsourcing arrangements may not contribute to the institution's safety and soundness. Furthermore, the agencies want to ensure that these arrangements with

---

<sup>1</sup> In summary, internal control is a process, brought about by an institution's board of directors, management and other personnel, designed to provide reasonable assurance that the institution will achieve the following internal control objectives: efficient and effective operations, including safeguarding of assets; reliable financial reporting; and, compliance with applicable laws and regulations. Internal control consists of five components that are a part of the management process: control environment, risk assessment, control activities, information and communication, and monitoring activities. The effective functioning of these components is essential to achieving the internal control objectives.

<sup>2</sup> For national banks, Appendix A to Part 30; for state member banks, Appendix D to Part 208; for state nonmember banks, Appendix A to Part 364; for savings associations, Appendix A to Part 570.

outsourcing vendors do not leave directors and senior managers with the impression that they have been relieved of their responsibility for maintaining an effective system of internal control and for overseeing the internal audit function.

This policy statement sets forth some characteristics of sound practices for the internal audit function and the use of outsourcing vendors for audit activities. In addition, it provides guidance on how these outsourcing arrangements may affect an examiner's assessment of internal control. It also discusses the effect these arrangements may have on the independence of an external auditor who also is providing internal audit services to an institution. Finally, this statement provides guidance to examiners concerning their reviews of internal audit functions and related matters. This policy statement applies to bank holding companies and their subsidiaries, FDIC-insured banks and savings associations, and U.S. operations of foreign banking organizations.

## THE INTERNAL AUDIT FUNCTION

### Director and Senior Management Responsibilities

The board of directors and senior management are responsible for having an effective system of internal control – including an effective internal audit function – and for ensuring that the importance of internal control is understood and respected throughout the institution. This overall responsibility cannot be delegated to anyone else. They may, however, delegate the design, implementation and monitoring of specific internal controls to lower-level management and the testing and assessment of internal controls to others. In discharging their responsibilities, directors and senior management should have reasonable assurance that the system of internal control prevents or detects inaccurate, incomplete or unauthorized transactions; deficiencies in the safeguarding of assets; unreliable financial and regulatory reporting; and deviations from laws, regulations, and the institution's policies.

Some institutions have chosen to rely on so-called “management self-assessments” or “control self-assessments,” wherein business line managers and their staff evaluate the performance of internal controls within their purview. Such reviews help to underscore management's responsibility for internal control, but they are not impartial. Directors and senior managers who rely too much on these reviews may not learn of control weaknesses until they have become costly problems – particularly if directors are not intimately familiar with the institution's operations. Therefore, institutions generally should also have their internal controls tested and assessed by units without business-line responsibilities, such as internal audit groups.

Directors should be confident that the internal audit function meets the demands posed by the institution's current and planned activities. Directors and senior managers should ensure that the following matters are reflected in their internal audit function.

*Structure.* Careful thought should be given to placement of the audit function in the institution's management structure. The function should be positioned so that directors have confidence that the internal audit function will perform its duties with impartiality and not be unduly influenced by managers of day-to-day operations. Accordingly, the manager of internal audit should report directly to

---

the board of directors or its audit committee, which should oversee the internal audit function.<sup>3</sup> The board or its audit committee should develop objective performance criteria to evaluate the work of the internal audit function.<sup>4</sup>

*Management, staffing, and audit quality.* The directors should assign responsibility for the internal audit function to a member of management (hereafter referred to as the manager of internal audit or internal audit manager) who understands the function and has no responsibilities for operating the business. The manager of internal audit should be responsible for control risk assessments, audit plans, audit programs and audit reports.

- A control risk assessment (or risk assessment methodology) documents the internal auditor's understanding of the institution's significant business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line and potential risk due to control deficiencies. They should be updated as needed to reflect changes to the system of internal control or work processes, and to incorporate new lines of business.
- The audit plan is based on the control risk assessment and includes a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.
- An audit program describes the objectives of the audit work and lists the procedures that will be performed during each internal audit review.
- An audit report generally presents the purpose, scope and results of the audit, including findings, conclusions and recommendations. Work papers should be maintained that adequately document the work performed and support the audit report.

The manager of internal audit should oversee the staff assigned to perform the internal audit work and should establish policies and procedures to guide the audit staff.<sup>5</sup> The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and assess whether internal controls are effective. Institutions should consider conducting their internal audit activities in accordance with professional standards, such as the Institute for Internal Auditors' (IIA) Standards for the Professional Practice of Internal Auditing. These standards address the independence, professional proficiency, scope of work, performance of audit work, and management of internal audit.

---

<sup>3</sup> Institutions subject to Section 36 of the FDI Act must maintain independent audit committees (i.e., comprised of directors that are not members of management). For institutions not subject to an audit committee requirement, the board of directors can fulfill the audit committee responsibilities discussed in this policy statement.

<sup>4</sup> For example, the performance criteria could include the timeliness of each completed audit, comparison of overall performance to plan, and other measures.

<sup>5</sup> The form and content of policies and procedures should be consistent with the size and complexity of the department and the institution: many policies and procedures may be communicated informally in small internal audit departments, while many larger departments require more formal and comprehensive written guidance.

*Scope.* The frequency and extent of internal audit review and testing should be consistent with the nature, complexity, and risk of the institution's on- and off-balance-sheet activities. At least annually, the audit committee should review and approve the internal audit manager's control risk assessment and the scope of the audit plan, including how much the manager relies on the work of an outsourcing vendor. It should also periodically review internal audit's adherence to the audit plan. The audit committee should consider requests for expansion of basic internal audit work when significant issues arise or when significant changes occur in the institution's environment, structure, activities, risk exposures, or systems.<sup>6</sup>

*Communication.* To properly discharge their responsibility for internal control, directors and senior management should foster forthright communications and critical examination of issues so that they will have knowledge of the internal auditor's findings and operating management's solutions to identified internal control weaknesses. Internal auditors should report internal control deficiencies to the appropriate level of management as soon as they are identified. Significant matters should be promptly reported directly to the board of directors (or its audit committee) and senior management. In periodic meetings with management and the manager of internal audit, the audit committee should assess whether internal control weaknesses or other exceptions are being resolved expeditiously by management. Moreover, the audit committee should give the manager of internal audit the opportunity to discuss his or her findings without management being present.

## U.S. Operations of Foreign Banking Organizations

The internal audit function of a foreign banking organization (FBO) should cover its U.S. operations in its risk assessments, audit plans, and audit programs. The internal audit of the U.S. operations normally is performed by its U.S. domiciled audit function, head-office internal audit staff, or some combination thereof. Internal audit findings (including internal control deficiencies) should be reported to the senior management of the U.S. operations of the FBO and the audit department of the head office. Significant, adverse findings also should be reported to the head office's senior management and the board of directors or its audit committee.

## Small Financial Institutions

An effective system of internal control, including an independent internal audit function, is a foundation for safe and sound operations, regardless of an institution's size. As discussed previously in this policy statement, Section 39 of the FDI Act requires each institution to have an internal audit function that is appropriate to its size and the nature and scope of its activities. The procedures assigned to this function should include adequate testing and review of internal controls and information systems.

It is management's responsibility to carefully consider the level of auditing that will effectively monitor the internal control system after taking into account the audit function's costs and benefits. For many institutions that have reached a certain size or complexity of operations, the benefits derived from a

---

<sup>6</sup> Major changes in an institution's environment and conditions may compel changes to the internal control system and also warrant additional internal audit work. These include: (a) new management; (b) areas or activities experiencing rapid growth; (c) new lines of business, products or technologies; (d) corporate restructurings, mergers and acquisitions; and (e) expansion or acquisition of foreign operations (including the impact of changes in the related economic and regulatory environments.)



full-time manager of internal audit or auditing staff more than outweigh its costs. However, for certain smaller institutions with few employees and less complex operations, these costs may outweigh the benefits. Nevertheless, a small institution without an internal auditor can ensure that it maintains an objective internal audit function by implementing a system of independent reviews of key internal controls. The employee conducting the review of a particular function should be independent of the function and able to report findings directly to the board or audit committee.

## INTERNAL AUDIT OUTSOURCING ARRANGEMENTS <sup>7</sup>

### Examples of Arrangements

An outsourcing arrangement is a contract between the institution and an outsourcing vendor to provide internal audit services. Outsourcing arrangements take many forms and are used by institutions of all sizes. The services under contract can be limited to helping internal audit staff in an assignment for which they lack expertise. Such an arrangement is typically under the control of the institution's manager of internal audit and the outsourcing vendor reports to him or her. Institutions often use outsourcing vendors for audits of areas requiring more technical expertise, such as those of electronic data processing and capital markets activities. Such uses are often referred to as "internal audit assistance" or "audit co-sourcing."

Some outsourcing arrangements may require an outsourcing vendor to perform virtually all internal audit work. Under such an arrangement, the institution may maintain a manager of internal audit and a very small internal audit staff. The outsourcing vendor assists staff in determining risks to be reviewed, recommends and performs audit procedures as approved by the internal audit manager, and reports its findings jointly with the internal audit manager to either the full board or its audit committee.

### Additional Considerations for Internal Audit Outsourcing Arrangements

Even when outsourcing vendors provide internal audit services, the board of directors and senior managers of an institution are responsible for ensuring that the system of internal control (including the internal audit function) operates effectively. When negotiating the outsourcing arrangement with an outsourcing vendor, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. The outsourcing arrangement should not increase the risk that a breakdown of internal control can occur.

To clearly set forth its duties from those of the outsourcing vendor, the institution should have a written contract, often referred to as an engagement letter. At a minimum, the contract should:

- Set the scope and frequency of work to be performed by the vendor;
- Set the manner and frequency of reporting to senior management and directors about the status of contract work;

---

<sup>7</sup> The guidance in the preceding section of this policy statement ("The Internal Audit Function") also applies to internal audit outsourcing arrangements.

- 
- Establish the protocol for changing the terms of the service contract, especially for expansion of audit work if significant issues are found;
  - State that internal audit reports are the property of the institution, that the institution will be provided with any copies of the related work papers it deems necessary, and that employees authorized by the institution will have reasonable and timely access to the work papers prepared by the outsourcing vendor;
  - Specify the locations of internal audit reports and the related work papers;
  - State that examiners will be granted immediate and full access to the internal audit reports and related work papers prepared by the outsourcing vendor;
  - Prescribe the method for determining who bears the cost of consequential damages; arising from errors, omissions and negligence; and
  - State that outsourcing vendors that are subject to the independence guidance below will not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee.

*Management.* Directors and senior management should ensure that the outsourced internal audit function is competently managed. For example, larger institutions should employ sufficient competent staff members in the internal audit department to assist the manager of internal audit in overseeing the outsourcing vendor.

*Communication.* Communication between the internal audit function and directors and senior management should not diminish because the bank engages an outsourcing vendor. All work by the outsourcing vendor should be well documented and all findings of control weaknesses should be promptly reported to the institution's manager of internal audit. Decisions not to report the outsourcing vendor's findings to directors and senior management should be the mutual decision of the internal audit manager and the outsourcing vendor. In deciding what issues should be brought to the board's attention, the concept of "materiality," as the term is used in financial 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.

*Vendor Competence.* Before entering an outsourcing arrangement the institution should perform enough due diligence to satisfy itself that the outsourcing vendor has sufficient staff qualified to perform the contracted work. Because the outsourcing arrangement is a personal services contract, the institution's internal audit manager should have confidence in the competence of the staff assigned by the outsourcing vendor and receive prior notice of staffing changes. Throughout the outsourcing arrangement, management should ensure that the outsourcing vendor maintains sufficient expertise to perform effectively its contractual obligations.

*Contingency Planning.* When an institution enters into an outsourcing arrangement (or significantly changes the mix of internal and external resources used by internal audit), it increases its operating risk. Because the arrangement might be suddenly terminated, the institution should have a contingency plan

---

to mitigate any significant discontinuity in audit coverage, particularly for high risk areas. Planning for a successor to the prospective outsourcing vendor should be part of negotiating the latter's service contract.

### Independence of the External Auditor

*This section of the policy statement applies only to an outsourcing vendor who is a certified public accountant (CPA) and who performs a financial statement audit or some other service for the institution that requires independence under AICPA rules.<sup>8</sup>*

Many institutions engage certified public accounting firms to audit their financial statements and furnish other attestation services requiring independence. A certified public accounting firm that provides other services for its client (such as consulting, benefits administration or acting as an outsourcing vendor) risks compromising the independence necessary to perform attestation services. The professional ethics committee of the American Institute of Certified Public Accountants (AICPA) has issued rulings and interpretations specifically addressing whether a certified public accountant that furnishes both audit outsourcing and external audit or other attestation services to a client can still be considered independent.<sup>9</sup>

Section 36 of the FDI Act and associated regulations require management of every insured depository institution with total assets of at least \$500 million to obtain an annual audit of its financial statements by an independent public accountant, report to the banking agencies on the effectiveness of the institution's internal controls over financial reporting and on the institution's compliance with designated laws and regulations (management report), and obtain a report from an external auditor attesting to management's assertion about these internal controls (internal control attestation report). In order to satisfy these requirements, the institution's board of directors must select an external auditor that will satisfy the independence requirements established by the AICPA, and relevant requirements and interpretations of the Securities and Exchange Commission.

Questions have been raised about whether external auditors who perform an audit of the institution's financial statements or provide any other service that requires independence can also perform internal audit services and still be considered independent. The federal banking agencies are concerned that outsourcing arrangements may involve activities that compromise, in fact or appearance, the independence of an external auditor.

The AICPA has issued guidance to CPAs (Interpretation 101-13 and related rulings) on independence that addresses these issues. Under Interpretation 101-13, the CPA's performance of services required by the outsourcing arrangement "would not be considered to impair independence with respect to [an institution] for which the [CPA] also performs a service requiring independence, provided that [the CPA or the CPA's firm] does not act or appear to act in a capacity equivalent to a member of [the

---

<sup>8</sup> Although outsourcing arrangements involving CPAs who are not performing external audit or attestation services for a client are not subject to this independence guidance, they are subject to the other sections of this policy statement.

<sup>9</sup> In May 1997, the AICPA and the Securities and Exchange Commission announced the formation of the independence Standards Board (ISB), a private-sector body intended to establish independence standards for auditors of public companies. Any future standards established by the ISB should be considered in initiating or evaluating outsourcing arrangements with CPAs.

institution's] management or as an employee." The interpretation lists activities that would be considered to compromise a CPA's independence. Included are activities that involve the CPA "authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the client."<sup>10</sup>

Also, the AICPA's Ruling No. 103 sets forth three criteria for evaluating the independence of a CPA who concurrently provides internal audit outsourcing services and the internal control attestation report under Section 36 of the FDI Act. One criterion requires that management "does not rely on [the CPA's] work as the primary basis for its assertion and accordingly has (a) evaluated the results of its ongoing monitoring procedures built into the normal recurring activities of the entity (including regular management and supervisory activities) and (b) evaluated the findings and results of the [CPA's] work and other separate evaluations of controls, if any." Accordingly, a CPA's independence would be impaired if the CPA provides the primary support for management's assertion on the effectiveness of internal control over financial reporting. A copy of the interpretation and rulings is attached to this policy statement.

*Agencies' Views on Independence.* The agencies believe that other actions compromise independence in addition to those in Interpretation 101-13. Such actions include:<sup>11</sup>

- Contributing in a decision-making capacity or otherwise actively participating (e.g., advocating positions or actions rather than merely advising) in committees, task forces, and meetings that determine the institution's strategic direction; and
- Contributing in a decision-making capacity to the design, implementation, and evaluation of new products, services, internal controls or software that are significant to the institution's business activities.

---

<sup>10</sup> Other examples of outsourcing activities that would compromise a CPA's independence that are listed in Interpretation 101-13 include:

- Performing ongoing monitoring activities or control activities (i.e., reviewing loan originations as part of the client's approval process or reviewing customer credit information as part of the customer's sales authorization process) that affect the execution of transactions or ensure that transactions are properly executed, accounted for, or both and performing routine activities in connection with the client's operating or production processes that are equivalent to those of an ongoing compliance or quality control function;
- Reporting to the board of directors or audit committee on behalf of management or the individual responsible for the internal audit function;
- Preparing source documents on transactions;
- Having custody of assets;
- Approving or being responsible for the overall internal audit work plan, including the determination of the internal audit risk and scope, project priorities, and frequency of performance of audit procedures;
- Being connected with the client in any capacity equivalent to a member of client management or as an employee (for example, being listed as an employee in client directories or other client publications, permitting himself or herself to be referred to by title or description as supervising or being in charge of the client's internal audit function, or using the client's letterhead or internal correspondence forms in communications).

<sup>11</sup> The agencies believe that this guidance is consistent with the AICPA interpretation.

## EXAMINATION GUIDANCE

### Review of the Internal Audit Function and Outsourcing Arrangements

Examiners should have full and timely access to an institution's internal audit resources, including personnel, work papers, risk assessments, work plans, programs, reports, and budgets. A delay may require examiners to widen the scope of their examination work and may subject the institution to follow-up supervisory actions.

Examiners will assess the quality and scope of the internal audit work, regardless of whether it is performed by the institution's employees or by an outsourcing vendor. Specifically, examiners will consider whether:

- The board of directors (or audit committee) promotes the internal audit manager's impartiality and independence by having him or her directly report audit findings to it;
- The internal audit function's risk assessment, plans and programs are appropriate for the institution's activities;
- The internal audit function is adequately managed to ensure that audit plans are met, programs are carried out, and results of audits are promptly communicated to interested managers and directors;
- The institution has promptly responded to identified internal control weaknesses;
- Management and the board of directors use reasonable standards when assessing the performance of internal audit;
- The internal audit plan and program have been adjusted for significant changes in the institution's environment, structure, activities, risk exposures or systems;
- The activities of internal audit are consistent with the long-range goals of the institution and are responsive to its internal control needs; and
- The audit function provides high-quality advice and counsel to management and the board of directors on current developments in risk management, internal control, and regulatory compliance.

The examiner should assess the competence of the institution's internal audit staff and management by considering the education and professional background of the principal internal auditors.

*Additional Aspects of the Examiner's Review of Outsourcing Arrangements.* Examiners should also determine whether:

- The arrangement maintains or improves the quality of the internal audit function and the institution's internal control;

- Key employees of the institution and the outsourcing vendor clearly understand the lines of communication and how any internal control problems or other matters noted by the outsourcing vendor are to be addressed;
- The scope of work is revised appropriately when the institution's environment, structure, activities, risk exposures or systems change significantly;
- The directors have ensured that the outsourced internal audit function is effectively managed by the institution;
- The arrangement with the outsourcing vendor compromises its role as external auditor; and
- The institution has performed sufficient due diligence to satisfy itself of the vendor's competence before entering into the outsourcing arrangement and has adequate procedures for ensuring that the vendor maintains sufficient expertise to perform effectively throughout the arrangement.

If the examiner's evaluation of the outsourcing arrangement indicates that the outsourcing arrangement has diminished the quality of the institution's internal audit function, the examiner should consider adjusting the scope of the examination. The examiner also should bring that matter to the attention of senior management and the board of directors and consider it in the institution's management and composite ratings.

### Concerns about Auditor Independence

When an examiner's initial review of an outsourcing arrangement raises doubts about the external auditor's independence, the examiner first should ask the institution and the external auditor to demonstrate that the arrangement has not compromised the auditor's independence. If the examiner's concerns are not adequately addressed, the examiner should discuss the matter with appropriate agency staff.

If the agency's staff concurs that the independence of the external auditor appears to be compromised, the examiner will discuss his or her findings and the actions the agency may take with the institution's senior management, board of directors (or audit committee), and the external auditor. These actions may include referring the external auditor to the state board of accountancy and the AICPA for possible ethics violations, and barring the external auditor from engagements with regulated institutions. Moreover, the agency may conclude that the organization's external auditing program is inadequate and that it does not comply with auditing and reporting requirements, including Section 36 of the FDI Act and related guidance and regulations.

---

**AICPA PROFESSIONAL RULINGS AND INTERPRETATIONS REFERENCED IN THE INTERAGENCY POLICY STATEMENT****RULINGS UNDER RULE OF CONDUCT 101****103. Member Providing Attest Report on Internal Controls**

*Question* - If a member or a member's firm (member) provides extended audit services for a client in compliance with interpretation 101- 13 [ET section 101.15], would the member be considered independent in the performance of an attestation engagement to report on the client's assertion regarding the effectiveness of its internal control over financial reporting?

*Answer* - Independence would not be impaired with respect to the issuance of such a report if all of the following conditions are met:

1. The member's activities have been limited in a manner consistent with interpretation 101- 13 [ET section 101.15].
2. Management has assumed responsibility to establish and maintain internal control.
3. Management does not rely on the member's work as the primary basis for its assertion and accordingly has (a) evaluated the results of its ongoing monitoring procedures built into the normal recurring activities of the entity (including regular management and supervisory activities) and (b) evaluated the findings and results of the member's work and other separate evaluations of controls, if any.

**104. Member Providing Operational Auditing Services**

*Question* - As part of an extended audit engagement, a member or member's firm (member) may be asked to review certain of the client's business processes, as selected by the client, for how well they function, their efficiency, or their effectiveness. For example, a member may be asked to assess whether performance is in compliance with management's policies and procedures, to identify opportunities for improvement, and to develop recommendations for improvement or further action for management consideration and decision-making. Would the member's independence be considered to be impaired in performing such a service?

*Answer* - The member's independence would not be considered to be impaired provided that during the course of the review the member does not act or appear to act in a capacity equivalent to that of a member of client management or of an employee. The decision as to whether any of the member's recommendations will be implemented must rest entirely with management.

**105. Frequency of Performance of Extended Audit Procedures**

*Question* - In providing extended audit services, would the frequency with which a member performs an audit procedure impair the member's independence?

*Answer* - The independence of the member or member's firm would not be considered to be impaired provided that the member's activities have been limited in a manner consistent with interpretation 101-13 [ET section 101.15] and the procedures performed constituted separate evaluations of the effectiveness of the ongoing control and monitoring activities/procedures that are built into the client's normal recurring activities.

## INTERPRETATION 101-13 UNDER RULES OF CONDUCT 101: EXTENDED AUDIT SERVICES

**.15 101-13 - Extended audit services.** A member or a member's firm (the member) may be asked by a client, for which the member performs a professional service requiring independence, to perform extended audit services. These services may include assistance in the performance of the client's internal audit activities and/or an extension of the member's audit service beyond the requirements of generally accepted auditing standards (hereinafter referred to as "extended audit services").

A member's performance of extended audit services would not be considered to impair independence with respect to a client for which the member also performs a service requiring independence, provided that the member or his or her firm does not act or does not appear to act in a capacity equivalent to a member of client management or as an employee.

The responsibilities of the client, including its board of directors, audit committee, and management, and the responsibilities of the member, as described below, should be understood by both the member and the client. It is preferable that this understanding be documented in an engagement letter that indicates that the member may not perform management functions, make management decisions, or act or appear to act in a capacity equivalent to that of an employee.

A member should be satisfied that the client understands its responsibility for establishing and maintaining internal control and directing the internal audit function, if any. As part of its responsibility to establish and maintain internal control, management monitors internal control to assess the quality of its performance over time. Monitoring can be accomplished through ongoing activities, separate evaluations or a combination of both. Ongoing monitoring activities are the procedures designed to assess the quality of internal control performance over time and that are built into the normal recurring activities of an entity and include regular management and supervisory activities, comparisons, reconciliations and other routine actions. Separate evaluations focus on the continued effectiveness of a client's internal control. A member's independence would not be impaired by the performance of separate evaluations of the effectiveness of a client's internal control, including separate evaluations of the client's ongoing monitoring activities.

The member should understand that, with respect to the internal audit function, the client is responsible for –

- Designating a competent individual or individuals, preferably within senior management, to be responsible for the internal audit function.
- Determining the scope, risk and frequency of internal audit activities, including those to be performed by the member providing extended audit services.



- 
- Evaluating the findings and results arising from the internal audit activities, including those performed by the member providing extended audit services.
  - Evaluating the adequacy of the audit procedures performed and the findings resulting from the performance of those procedures by, among other things, obtaining reports from the member.

The member should be satisfied that the board of directors and/or audit committee is informed of roles and responsibilities of both client management and the member with respect to the engagement to provide extended audit services as a basis for the board of directors and/or audit committee to establish guidelines for both management and the member to follow in carrying out these responsibilities and monitoring how well the respective responsibilities have been met.

The member should be responsible for performing the audit procedures in accordance with the terms of the engagement and reporting thereon. The day-to-day performance of the audit procedures should be directed, reviewed, and supervised by the member. The report should include information that allows the individual responsible for the internal audit function to evaluate the adequacy of the audit procedures performed and the findings resulting from the performance of those procedures. This report may include recommendations for improvements in systems, processes, and procedures. The member may assist the individual responsible for the internal audit function in performing preliminary audit risk assessments, preparing audit plans, and recommending audit priorities. However, the member should not undertake any responsibilities that are required, as described above, to be performed by the individual responsible for the internal audit function.

Performing procedures that are generally of the type considered to be extensions of the member's audit scope applied in the audit of the client's financial statements, such as confirming of accounts receivable and analyzing fluctuations in account balances, would not impair the independence of the member or the member's firm even if the extent of such testing exceeds that required by generally accepted auditing standards. The following are examples of activities that, if performed as part of an extended audit service, would be considered to impair a member's independence:

- Performing ongoing monitoring activities or control activities (for example, reviewing loan originations as part of the client's approval process or reviewing customer credit information as part of the customer's sales authorization process) that affect the execution of transactions or ensure that transactions are properly executed, accounted for, or both, and performing routine activities in connection with the client's operating or production processes that are equivalent to those of an ongoing compliance or quality control function.
- Determining which, if any, recommendations for improving the internal control system should be implemented.
- Reporting to the board of directors or audit committee on behalf of management or the individual responsible for the internal audit function.
- Authorizing, executing, or consummating transactions or otherwise exercising authority on behalf of the client.

- Preparing source documents on transactions.
- Having custody of assets.
- Approving or being responsible for the overall internal audit work plan including the determination of the internal audit risk and scope, project priorities and frequency of performance of audit procedures.
- Being connected with the client in any capacity equivalent to a member of client management or as an employee (for example, being listed as an employee in client directories or other client publications, permitting himself or herself to be referred to by title or description as supervising or being in charge of the client's internal audit function, or using the client's letterhead or internal correspondence forms in communications).

The foregoing list is not intended to be all inclusive.

[Effective August 31, 1996]

AICPA Professional Standards

Copyright © 1996, American Institute of Certified Public Accountants, Inc.

---

**INTERNAL AUDITOR QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #:** >

**Institution Name:** >

**Examination As of Date:** >

---

The financial institution's internal auditor or person in charge of internal controls who does not have operational responsibilities should complete this questionnaire. An outside contractor or the internal audit department of an affiliate who performs internal control review functions for the financial institution may also complete this questionnaire.

Check here if the financial institution does not have an internal audit function: \_\_\_\_\_ If checked, stop here.

*The examiners will complete minimum procedures (indicated by a flag) if the institution does not have an independent internal audit function or there is a "no" response given below. Independent means that the staff responsible for internal audit does not have operational responsibilities and they report directly to the audit committee or board of directors. Minimum procedures are set forth in the Internal Control Program in Section 340, Internal Control. Examiners will note completed work with a work paper reference at the flag(s) below.*

The \_\_\_\_ internal auditor \_\_\_\_ outside contractor \_\_\_\_ internal audit department of an affiliate completed this questionnaire.

List the name, address, and telephone number of the primary contact at the institution and the name, address, telephone number, and email address for any persons outside the institution who prepared this report:

---

**INTERNAL AUDITOR QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**



**Docket #:** >  
**Institution Name:** >  
**Examination As of Date:** >

Yes      No

**Internal Control Department**

1. List the chief internal auditor’s name, any related professional designation(s), and number of years of financial institution and auditing experience.  
 \_\_\_\_\_
2. List the other employees in the internal audit department and the audit experience of each.  
 \_\_\_\_\_
3. How long has the chief auditor worked for the institution, and how long has this person held the present position?  
 \_\_\_\_\_
4. Whom does the chief auditor report to functionally? Administratively?  
 \_\_\_\_\_
5. Does the external CPA firm rely on work performed by the internal audit department in determining the extent of their compliance or substantive testing?      \_\_\_\_\_
6. Did the audit department discover any frauds or embezzlements since the last OTS examination? If yes, please attach information for review.      \_\_\_\_\_
7. Are work papers accessible for review by examiners?      \_\_\_\_\_

**General**







8.  Does the audit department test general ledger entries for appropriate support and approval?      \_\_\_\_\_
9.  Does the audit department review expense disbursements for appropriate support and approval?      \_\_\_\_\_

**INTERNAL AUDITOR QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >

**Institution Name:** >

**Examination As of Date:** >

		<u>Yes</u>	<u>No</u>
10.	 Does the audit department review procedures to determine that subsidiary accounts are reconciled promptly to the general ledger, including suspense accounts? (This can be as frequently as daily depending upon the volume and significance.)	_____	_____
11.	 On a test basis, do audit procedures include the review of the approval and documentation for entries to the books of the financial institution?	_____	_____
12.	Do audit procedures include a review of the institution assets, or assets securitized by the institution, that others hold or service?	_____	_____
13.	 Does the audit department balance a listing of assets others hold or service monthly, and confirm balances annually?	_____	_____
14.	 Do audit procedures include the review of insider and affiliated party transactions for proper documentation and approval?	_____	_____
<b>Cash and Cash Items</b>			
15.	 Do audit procedures include a review of internal controls in this area?	_____	_____
16.	State the audit frequency in this area for the main office and the branches.  _____		
17.	How frequently does the audit department perform surprise cash counts?  _____		
18.	Does the audit department trace cash items to their final disposition?	_____	_____
19.	How frequently do audit procedures require testing for adherence to established teller cash limits?  _____		
20.	 Do audit procedures require testing for adherence to dual control policies where applicable?	_____	_____

**INTERNAL AUDITOR QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As of Date:** >

	<u>Yes</u>	<u>No</u>
21.  Do audit procedures include review of the use of supervisory overrides relating to teller operations?	_____	_____
22. List the dates of the last audits in this area.  _____		
<b>Due From Banks</b>		
23.  Do audit procedures include a review of internal controls in this area?	_____	_____
24. State the audit frequency for this area.  _____		
25. Does the auditor request cut-off statements and canceled checks when auditing this area?	_____	_____
26. When auditing this area, which reconcilements are proved such as audit date, most recent, etc.?  _____		
27.  Does the audit department undertake a review to ensure that the institution reconciles all bank accounts when they receive the statement?	_____	_____
28.  Does the institution trace outstanding reconciliation items from the last audit to final disposition, noting unusual aging and number of reconciling items?	_____	_____
29. How frequently does the audit department review drafts for propriety?  _____		
30. Do audit procedures include tracing selected items from the general ledger to the source (originating department)?	_____	_____
31. List the dates of the last audits of this area.  _____		

**INTERNAL AUDITOR QUESTIONNAIRE  
Preliminary Examination Response Kit  
Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As of Date:** >

	<u>Yes</u>	<u>No</u>
<b>Investment Portfolio</b>		
32.  Do audit procedures include a review of internal controls in this area?	_____	_____
33. State the audit frequency for this area.  _____		
34. Does the audit department establish control over the vault(s) containing physical securities at the beginning of surprise audits (or announced audits)?	_____	_____
35.  Is there physical verification of the securities to the subsidiary ledger?	_____	_____
36.  Do audit procedures include reconciling the subsidiary ledger(s) to the general ledger control account(s) as of the audit date or a recent date?	_____	_____
37.  Do audit procedures include confirming securities held in safekeeping outside the institution?	_____	_____
38. Were all securities in safekeeping outside the institution confirmed during the last audit?	_____	_____
39. Do audit procedures include reviewing the par value of inventory for compliance with limits on authorized holdings?	_____	_____
40. What was the date of the last audit of this area?  _____		
<b>Demand Deposits</b>		
41.  Do audit procedures include a review of internal controls in this area?	_____	_____
42. State the audit frequency in this area.  _____		
43. Do audit procedures require confirmation of a sample of demand accounts including dormant accounts?	_____	_____

**INTERNAL AUDITOR QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As of Date:** >

	<u>Yes</u>	<u>No</u>
44. If the answer above is yes, are positive confirmations used?	_____	_____
45.  Do audit procedures require a review of dormant activity and compliance with the es-cheat laws currently in effect?	_____	_____
46.  On a test basis, do audit procedures require a review of returned and holdover items for propriety and evidence of subsequent clearance of material items?	_____	_____
47.  Do procedures provide for a review of the handling of uncollected funds and kiting?	_____	_____
48.  Do procedures provide for a review of director, officer, and employee accounts for large or unusual transactions relative to their salary?	_____	_____
49. List the last audit date for this area.  _____		

**Time Deposits**

50.  Do audit procedures include a review of internal controls in this area?	_____	_____
51. State the audit frequency in this area.  _____		
52. Do audit procedures require confirmation of a sample of time accounts including dormant accounts?	_____	_____
53. If the answer above is yes, are positive confirmations used?	_____	_____
54.  Do audit procedures require a review of dormant activity and compliance with the es-cheat laws currently in effect?	_____	_____
55. How frequently does the audit department test interest accrued and paid to accounts?	_____	_____
56. Does the audit department use audit software in the testing referred to in the question above?	_____	_____






**INTERNAL AUDITOR QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #:** >  
**Institution Name:** >  
**Examination As of Date:** >

		<u>Yes</u>	<u>No</u>
57.	List the last audit date for this area.  _____		
	<b>Loans</b>		
58.	Do audit procedures include a review of internal controls in this area?	_____	_____
59.	State the audit frequency in this area.  _____		
60.	Do audit procedures require confirmation of a sample of loan accounts?	_____	_____
61.	If the above is yes, are positive confirmations used?	_____	_____
62.	Does the audit department’s responsibilities include evaluating the adequacy of the loan loss reserves?	_____	_____
63.	On a test basis, does the audit department review the approvals for loan disbursements and charged-off loans?	_____	_____
64.	How frequently does the audit department test income and related accrued interest and unearned discount?	_____	_____
65.	Does the audit department use audit software in the testing referred to in the question above?	_____	_____
66.	Do audit procedures include a test check of the inventory of original notes, deeds of trust, car titles, and negotiable collateral for loans in the portfolio?	_____	_____
67.	List the last audit date for this area  _____		
	<b>Wire Transfers</b>		
68.	Do audit procedures include a review of internal controls in this area?	_____	_____

**INTERNAL AUDITOR QUESTIONNAIRE**  
**Preliminary Examination Response Kit**  
**Office of Thrift Supervision**

**Docket #: >**  
**Institution Name: >**  
**Examination As of Date: >**

	<u>Yes</u>	<u>No</u>
69. State the audit frequency in this area.  _____		
70.  Does the audit department test wire transfers to ensure timely verifications and reconciliations?	_____	_____
71.  Does the audit department undertake a review to ensure that wire transfer process involves independent parties?	_____	_____
72.  Does the audit department test wire transfers to ensure compliance with written procedures?	_____	_____
73. List the last audit date for this area  _____		

## Fraud and Insider Abuse

Fraud and insider abuse significantly contributed to many thrift failures during the late 1980s and early 1990s, and caused substantial losses at many others. Because of this, several federal agencies now work closely together to combat fraud and insider abuse at financial institutions.

The Interagency Bank Fraud Working Group includes the five federal banking agencies, the Department of Justice (DOJ), and the Federal Bureau of Investigation (FBI). Representatives from these government agencies work together to establish policies to improve interagency cooperation and to resolve criminal investigation and prosecution problems.

All the agencies now use a uniform interagency Suspicious Activity Report (SAR) form. This is a form that federally insured financial institutions use to report suspected violations of federal criminal law and suspicious transactions related to money laundering offenses and Bank Secrecy Act violations. In addition, all the federal banking regulators have regulations that require insured institutions and service corporations to file SARs.

---

### LINKS

---

 [Program](#)

---

 [Appendix A](#)

---

 [Appendix B](#)

DOJ maintains the Significant Referral Tracking System. This system tracks the progress of SARs that the federal financial regulators designate as most significant. The DOJ provides tracking of their progress in local U.S. Attorneys' Offices.

To facilitate these interagency efforts, OTS designates a criminal referral coordinators. Their function is to coordinate reports of suspected criminal activities and provide assistance to the FBI and DOJ in criminal investigations and prosecutions.

## FRAUD, INSIDER ABUSE, AND CRIMINAL MISCONDUCT

Fraud is the intentional misrepresentation of a material fact(s), or a deception, to secure unfair or unlawful gain at the expense of another. Either insiders or outsiders, or both acting in concert, can perpetrate fraud on financial institutions.

Every year, thrifts lose a significant amount of money due to insider abuse and criminal misconduct. The FBI estimates that insiders of financial institutions steal eight times more money than is stolen through bank robberies and burglaries.

The term insider abuse refers to a wide range of activities by officers, directors, employees, major shareholders, agents, and other controlling persons in financial institutions. The perpetrators intend to

benefit themselves or their related interests. Their actions include, but are not limited to, the following activities:

- Unsound lending practices, such as inadequate collateral and poor loan documentation.
- Excessive concentrations of credit to certain industries or groups of borrowers.
- Unsound or excessive loans to insiders or their related interests or business associates.
- Violations of civil statutes or regulations, such as legal lending limits or loans to one borrower.
- Violations of criminal statutes, such as fraud, misapplication of bank funds, or embezzlement.

In addition to criminal misconduct, insider abuse includes other actions or practices that may harm or weaken an institution, but that do not violate criminal statutes. While every criminal violation by an insider constitutes insider abuse, not all insider abuse constitutes criminal misconduct. In most problem financial institutions where regulators find insider abuse, they also find a variety of unsafe and unsound banking practices and mismanagement that may involve criminal acts. While a thin line often separates a criminal act from an abusive act, OTS has the responsibility and the authority to act against all insider abuse, whether criminal or not.

Many of the largest cases of financial institution fraud involved insiders. If the insider is in a key position, the amount of loss can be significant enough to cause the institution to fail. Often, these individuals perform criminal acts using subordinates who do not question their instructions. In some instances, however, the subordinates may be astute enough to know that what the insiders instructed them to do is questionable or wrong and may freely discuss the situation if the regulators simply inquire.

During formal and informal discussions with employees, you should listen carefully and be attuned to signals of possible illegal activity by others within the institution. Often, discovering fraud is a matter of talking with the right person who knows what is occurring. Inside abusers often start with small transactions, and engage in increasingly larger transactions as their confidence level rises. Because of this, the early detection of insider abuse is an essential element in limiting risks to the insurance fund.

Generally you should bring up fraud as part of another discussion. Once you have established some rapport, you should first ask, as appropriate to the person you are interviewing, general questions, and then more specific questions:

- What kind of history does the association have with fraud in general, including defalcations and employee thefts?
- During the examination, what specific areas should we examine to ensure that there are no major fraud problems?
- Has anyone else ever asked you to do something that you thought was illegal or unethical?

- If someone wanted to commit fraud against the association, what would be the easiest way to do it?
- Is the association in any kind of financial trouble that would motivate someone to commit fraud?
- Is anyone in any personal financial difficulty that you are aware of?
- Have you ever committed fraud against the company?

## Criminal Statutes

The following criminal statutes apply to financial fraud:

### *18 USC § 215*

Kickbacks and bribes. Section 215 makes it unlawful for any officer, director, employee, agent, or attorney to solicit, accept, or give anything of value with intent to corrupt, in connection with any transaction or business of any financial institution.

Significant Aspects:

- Intent to corrupt requires intent to receive a personal financial benefit or to direct to another person such benefit.
- Applies to noncustomer transactions, for instance, suppliers.
- Applies where a person makes a payment after the fact to reward another person for a prior act.
- Can apply where a third party receives the benefit if the intent is to influence the insider.

### *18 USC § 657*

Theft, embezzlement, or willful misapplication of an insured institution's funds by an officer, director, agent, or employee with intent to defraud the institution.

Significant Aspects:

- Applies to check kites, nominee borrowers, and in some cases unauthorized loans.
- Violation of internal policies, violation of regulations, and personal benefit to the insider.

## *18 USC § 1001*

Knowingly and willfully falsifying or concealing a material fact or making a false statement or making or using false writing knowing it to be false.

## *18 USC § 1006*

False entries and reports or statements. Includes material omissions, with intent to injure or defraud an insured institution or deceive an OTS regulator. The statute also covers an officer's, agent's, or employee's receipt of any benefits from an institution transaction with intent to defraud.

Significant Aspects:

- Misstatement should be material.
- Often used in conjunction with misapplication statutes such as 18 USC § 657.

## *18 USC § 1014*

False statement, oral or written (for instance, loan applications), made knowingly for the purpose of influencing OTS or any federally insured institution. False statements apply to any application, purchase agreement, commitment, loan (or any change or extension of same), including willfully overvaluing land, property, or security.

Significant Aspects:

- Usually used against borrowers for submitting false financial statements.
- Statute applies to all persons, not just insiders.

## *18 USC § 1344*

Bank fraud: A scheme or artifice to defraud a federally insured institution or take money, funds, credit, assets, security, or other property by misrepresentation.

Significant Aspects:

- Applies to most activities that are violations under the statutes.
- Generally must find deceit, trickery, deception, falsehood, or failure to provide information when there is an obligation to do so.

## *18 USC § 1517*

Obstructing an examination. It is a crime to corruptly obstruct or attempt to obstruct an examination of a financial institution.

Significant Aspects:

- The examination must be one that an agency of the United States, with examination jurisdiction, is conducting.

Applies to whoever corruptly obstructs or attempts to obstruct.

## *18 USC § 709*

This criminal statute applies restrictions on advertising and names used by non-federal persons or entities.

Significant Aspects:

- Prohibition, except where permitted by law, of the use of several words relating to federal entities without authority.
- Restrictions include the use, except where permitted by the laws of the United States, of the words national, Federal, United States, reserve, or deposit insurance as part of the business or firm name of a person, corporation, partnership, business trust, association, or other business entity engaged in the banking, loan, building and loan, brokerage, factorage, insurance, indemnity, savings or trust business.
- Restrictions also apply to many other words, acronyms, advertisements or representations.

## CONFLICTS OF INTEREST

There remains a continuing need for regulatory personnel to scrutinize all conflict of interest transactions in the context of OTS's Conflicts of Interest regulation § 563.200. You should, accordingly, comment on and request appropriate corrective action on any actual or apparent conflict of interest situation that adversely affects the institution, even though a regulation may not specifically address the conflict. You should also comment on and request appropriate corrective action whenever people involved in a conflict situation participate in or exercise an undue influence over the approval of the transactions.

## IMPORTANCE OF INTERNAL CONTROLS

Savings associations facing increased competition often consider implementing new strategies including cutting costs, offering different products, and pursuing other activities that have higher yields. While OTS recognizes that savings associations must adapt to changing business conditions, it is critically important that management maintain strong internal controls.

The following are some examples of unsafe, unsound, and sometimes fraudulent activities that have caused savings associations to suffer significant financial losses due to breakdowns in internal controls:

- Unauthorized and unsupervised overdrafts of customers' checking accounts.
- Unauthorized loans and falsified loan records.
- Employee embezzlements involving check kiting schemes.
- Unauthorized withdrawals from a correspondent account.
- Unreported teller shortages.

Inadequate internal controls also contribute to losses associated with a shift from traditional activities to higher risk commercial and consumer lending. In addition, in face of increasing competition and shrinking margins many associations desire to cut costs, particularly in areas not directly tied to income. Associations must direct expense control to areas that do not compromise critical policies and procedures governing internal controls.

### *Internal Control Regulatory Requirements*

The Federal Deposit Insurance Corporation Improvement Act of 1991 required the banking agencies to establish certain safety and soundness guidelines. Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness, includes a section on operational and managerial standards. Pursuant to the standards, each savings association must have internal controls and an internal audit appropriate to the size of the association and the nature and scope of its activities. Pursuant to FDIC regulation 12 CFR § 363.5, Audit Committees, insured depository institutions with total assets of \$500 million or more must have an audit committee composed of outside directors who are independent of management.

### *Internal Control System*

When determining the effectiveness of an association's internal control system, you must be particularly alert to the following situations:

- Management does not implement effective procedures to correct internal control deficiencies noted in reports prepared by the internal auditors or the independent accountants.
- Management scales back or suspends the internal audit function.
- The internal auditor has dual, operational responsibilities that compromise the internal audit function.
- The internal auditor reports to management instead of directly to the board of directors or an audit committee.



- The association's independent audit firm does not have banking audit experience. A similar problem may exist when a nationally recognized accounting firm assigns auditors to a savings association audit who are not familiar with banking procedures and practices.
- The association discontinues the annual independent accountant's audit.
- The association does not have proper controls in high-risk lending areas (this could be the result of poor policies, frequent exceptions to policy, or understaffing).
- The association engages in new lending activities with inadequate or unqualified staff.
- The association often deviates from board-approved policies without exception documentation.
- The association fails to effectively segregate duties and responsibilities among employees.
- The association fails to provide adequate reports to the board of directors.

#### *Internal Control System Critical Components*

There are a number of common critical components in internal control systems that are applicable to all savings associations. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a report<sup>1</sup> that identified five critical components of a good internal control framework:

- Control environment
- Risk assessment
- Control activities
- Accounting, information, and communication systems
- Self assessment.

COSO defines internal control as a process to achieve the following objectives:

- Effectiveness and efficiency of operations including safeguarding assets.
- Reliability of financial reporting.
- Compliance with applicable regulations.

---

<sup>1</sup> Savings associations may obtain the COSO "Internal Control – Integrated Framework" (Product code #990009) from the Order Department, American Institute of Certified Public Accountants, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881. Toll-free telephone 1-888-777-7077; FAX 1-800-362-5066.

Generally accepted auditing standards incorporate in the AICPA Statement on Auditing Standards No. 78, Consideration of Internal Control in a Financial Statement Audit, the common critical elements of internal control systems contained in COSO. OTS urges savings association directors and management to review at least the major concepts described in the COSO report or other recognized standards and compare them to their association's internal control systems. Good internal control processes are only effective if properly understood and strictly followed. The board of directors must establish internal control systems policy and properly monitor implementation of the policy. Management must properly implement internal control systems according to board policy. In addition, internal and external auditors should vigorously check the appropriateness and effectiveness of savings associations' internal controls. See Examination Handbook Section 340, Internal Control.

### Access to Savings Association Directors, Employees, Agents, and Books and Records

A number of federal statutes entitle you to prompt and unrestricted access to savings association directors, employees, agents, books, and records. In some instances, association management attempted to delay or limit your access to information with the intent to conceal fraud, derogatory information, or insider abuse. Such obstruction, however, more often occurs due to a lack of understanding by association personnel. In either case, you can usually promptly resolve access problems by reviewing the appropriate statutory requirements with association management. You must recognize obstruction and consider it a red flag indicating potentially serious problems, and take steps to prevent it.

#### *Tools to Prevent Examination Obstruction*

The following statutes and regulations grant you prompt and complete access to savings association directors, employees, agents, and books and records.

- 12 USC § 1464(d)(1)(B)(ii) requires associations to give you prompt and complete access to its officers, directors, employees, and agents, and to all relevant books, records, or documents of any type during an examination.
- 12 USC § 1464(d)(1)(B)(iii) requires associations to give you prompt and full access to all records and staff for regulatory purposes at all other times.
- 12 USC § 1467a(b)(4) provides you with authority to examine savings and loan holding companies.
- 12 USC § 1467a(b)(3), 12 CFR § 563.170(c) requires institutions and their holding companies to maintain complete records of their business and make them available to you wherever they are located.
- 12 USC § 1464(d)(7)(D)(i) and 1831v, and 12 CFR § 563.170(e) provides you with access to the records and staff of service providers unless the service provider is functionally regulated.

- 12 USC § 1464(d)(1)(B)(i), 1467a(b)(4) and 1831v allows you unrestricted access to records of affiliates (including holding company subsidiaries) whose affairs affect insured institutions, unless the affiliate is functionally regulated.

When appropriate, you should remind associations that OTS may use its enforcement tools to obtain management's compliance with these access provisions. These tools include cease and desist orders, removal and prohibition orders, and civil money penalty assessments. In addition, examination obstruction may subject management to criminal prosecution under 18 USC § 1517.

### *Red Flags of Examination Obstruction*

Recognizing and refusing to tolerate obstruction is critical to preparing an accurate report of examination. It is important that you promptly notify your EIC or field manager of an association's attempt to obstruct your examination. If you try to ignore it, the evasion generally gets worse, as do the problems concealed by the obstruction.

Appendix B of this handbook section consists of a number of examination obstruction questions and answers.

### Examples of Obstruction

- **Delaying Tactics.** Savings associations sometimes do not provide requested information within a reasonable time. For example, the association may tell you that:
  - The only staff member who knows the location of the records is unavailable right now – and continues to be unavailable.
  - An association employee urgently needs a particular computer with the necessary records for other purposes.
  - The records are off site and there will be a delay in obtaining them.

Your response should be polite but firm; under federal statutes, unreasonable delays are impermissible. 12 USC § 1464(d)(1)(B)(ii).

- **Screening Tactics.** Associations may try to prescreen the documents you need to review requiring that you request documents or staff in advance. The association's intent may be to review or sanitize requested documents before you see them. Screening is impermissible. 12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 563.170(c).
- **Alteration of Records.** Association employees may attempt to alter records before your review to prevent you from discovering significant losses, fraud, or insider abuse. The employees may remove key documents from files, destroy records, or create required records (known as file stuffing). Two associations used these illegal tactics recently and criminal prosecutions followed. If you suspect records alteration, notify your EIC, field manager, or regional counsel. 18 USC §§ 1005 and 1006.

- **Removal of Records.** In several notorious cases, management removed important documents from association offices and hid them off site from examiners. You can only discover this conduct when you remain alert to the fact that obstruction may be occurring, and persistently follow up on employee comments and cross references to missing documents in other files. Removal of records violates several of the civil and criminal statutes cited above. If you suspect that this has occurred, you should notify your EIC, field manager, or regional counsel of your concerns.
- **Withholding Information based on Assertions of Privilege.** Associations, their attorneys, or their accountants may attempt to prevent you from accessing documents based on assertions of privilege or confidentiality. Because rulings on privilege claims can turn on specific facts, you should consult with your regional counsel whenever an association raises privilege claims. Generally, associations cannot properly use these assertions to bar you from attending executive board of director sessions or reviewing minutes of its meetings, including draft minutes. These assertions also may not prevent you from reviewing records of the association's operations, such as documents relating to loans that may be the subject of ongoing litigation between the association and third parties. The documents may be in the offices of the association's litigation counsel. You are entitled to review such documents wherever they are. 12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 563.170(c).
- **Attacks on your credibility.** Associations sometimes attempt to neutralize negative examination findings by attacking the credibility of individual examiners. Your best defense to this tactic is prevention. Use good judgment, comply with OTS policy, and make it a practice to have another examiner present during important or potentially hostile meetings with association employees.

### Stopping Examination Obstruction

You must promptly stop examination obstruction. We have found repeatedly that obstruction is a red flag for a variety of more serious problems. You cannot always identify and address these serious problems, however, until the association stops the obstruction.

Whenever you meet any of the types of obstruction noted above, you should immediately discuss the problem with senior management and seek a quick resolution of what could be a simple misunderstanding. You should explain to senior management the statutory basis for gaining access to all records. If you do not obtain access or if the association does not resolve the situation, you should inform your EIC or field manager. They will work with you, the ARD, and the regional counsel to address the problem. Any continued obstruction will involve other attorneys of the Chief Counsel's office as appropriate.

The following are several tools available for a prompt and complete remedy. The right response depends on the type and seriousness of the obstruction you meet and the Chief Counsel's suggestions as to the best way to proceed.

- Reviewing with the association's board of directors the applicable statutes that compel prompt and complete access of records and politely insisting on compliance. This course might involve arranging a meeting of the board with the field manager, ARD, RD, and/or regional counsel.
- Delivering a supervisory letter instructing the association to promptly comply with examiner requests for information or face formal enforcement action.
- Filing in the local United States District Court for an Order requiring that the association provide the requested information immediately. 12 USC § 1464(d)(1)(B)(iv).
- Issuing a temporary cease and desist order requiring that inaccurate or incomplete records be restored immediately to a complete and accurate state. 12 USC § 1818(c)(3)(A).
- In extreme cases, or where OTS has exhausted other remedies, appointing a conservator or receiver based on the association's concealment of records and obstruction of the examination. 12 USC § 1821(c)(5)(E).
- Where appropriate, or in conjunction with the remedies listed above, filing a suspicious activity report to the Department of Justice. Such filings may be for obstructing an examination, making false entries to defraud the association or deceive regulators, or concealing assets from an association's conservator, receiver, or liquidating agent. These illegal actions are subject to 18 USC §§ 1005, 1006, 1517, and 1032.

## DETECTING FRAUD AND INSIDER ABUSE

Because perpetrators do not always carefully plan and discreetly carry out fraud, if you are alert to certain warning signs you may be able to detect it. It is essential, however, that you are knowledgeable of the warning signs and are alert to circumstances where fraud may exist, either by insiders or outsiders. Once you suspect fraud you should thoroughly investigate the circumstances surrounding a suspected activity.

The primary problem that you face in detecting fraud is the limited time and resources available to conduct an examination. Certainly, if you are aware of it and it is material, you should devote the time necessary to determine the appropriate action. However, when you only mildly suspect it, such as with a hunch, it is difficult to justify expanding the examination scope. To assist you in assessing an institution's risk of fraud, this section attaches a Fraud Risk Evaluation Form ([Appendix A](#)) and includes the following subsection: Red Flags of Fraud and Insider Abuse. When you consider the risk of fraud to be high you may expand your examination scope in the appropriate areas.

You must be alert to situations that may be conducive to fraud and insider abuse. If a situation exists where an officer or employee is able to control a sizable transaction from beginning to completion, you should notify the board of directors. The board should immediately correct the situation. You should not think of internal control weaknesses, poor loan documentation, improper internal audit reporting relationships, etc., only as technical violations, but also as potential opportunities for large frauds. Such

weaknesses should receive appropriate treatment in the report of examination and should result in effective supervisory action.

### Red Flags of Fraud and Insider Abuse

Experience has taught OTS staff that certain common elements are often present in cases of fraud and insider abuse. The following listings are warning signs of possible fraud and insider abuse:

#### *General*

- Dominant officer with control over the institution or a critical operational area.
- Internal audit restrictions or unusual reporting relationships (the internal auditor not reporting directly to the board or audit committee).
- Lack of written or inadequately written policies.
- Lack of adherence to written policies.
- Unusual or lavish fixed assets (for example, aircraft or art work).
- Management attempts to unduly influence examination or audit findings.
- Material internal control deficiencies.
- Frequent changes of auditors.
- High internal audit department turnover.
- Alteration of records.
- Withholding of records.
- Delaying tactics in providing documents or records.
- Large transactions with small out-of-town banks.
- Ownership or control vested in a small group.
- Difficulty in determining who is in control.
- Overly complex organizational structure, managerial lines of authority, or contractual arrangements without apparent business purpose.
- Inaccurate, inadequate, or incomplete board reports.

- Discontinuation of key internal reports.
- No vacation taken by employee or officer.

## *Management Level*

- Routinely contests exam findings by filing appeals, complaining to congresspersons, or directly or indirectly contacting agency officials.
- Routinely accuses you of being unfair, acting overzealously, or making errors.
- Fails to provide actual documents – only provides copies.
- Hires ex-agency officials when faced with enforcement actions.
- High turnover of officials.
- Motivation to engage in fraudulent financial reporting – significant portion of management's compensation is contingent upon aggressive targeted financial achievements, stock prices, or earnings.
- Use of aggressive accounting practices or tax-motivated behavior.
- High degree of competition in the community accompanied by declining margins of profit or customer demand.

## *Exam Level*

- Inability to generate cash flows from operations.
- Assets, liabilities, revenues, or expenses based on significant estimates that involve subjective judgments or uncertainties.
- Unusually rapid growth in comparison to other institutions.
- High vulnerability to interest rate changes.
- Inadequate monitoring of significant controls.
- Lack of timely and appropriate documentation for transactions.
- Significant unexplained items on reconciliations.
- Falsified bank documents.

- Weak loan administration and out of balance loan accounts.
- Repeated regulatory violations including significant Thrift Financial Report violations year after year.
- Significant related party transactions not in the ordinary course of business.
- Significant bank accounts in tax haven jurisdictions.
- Weak internal controls and risk management such as, inadequate overall internal control design, inadequate procedures to assess and apply accounting principles, absence of controls for certain transaction activities, evidence that a system fails to provide accurate output, or evidence of design flaws, among others.
- Known criminal referrals.

### *Red Flags of Lending Abuse*

- Poorly documented loans and appraisals.
- Lack of an acceptable past due or watch list.
- Lack of, or unsigned, borrower financial statements.
- Questionable loan disbursement transactions.
- Loan funds disbursed to a third party.
- Corporate loans with no endorsements or guarantors.
- Large pay-down of problem loans prior to an audit or examination.
- Large overdrafts.
- Refinancing of debt in a different department.
- Loans secured by flipped collateral.
- Nominee loans.
- Loans of unusual size or with unusual interest rates or terms.
- Loans with unusual, questionable, or no collateral.
- Loan review restrictions.



- Questionable, out-of-territory loans.
- Evergreen loans (loans continuously extended or modified).
- A considerable number or amount of insider loans.
- Construction draws with no or inadequate inspection reports.
- Construction inspections conducted by unauthorized or inappropriate persons.
- Market study on proposed project not on file.
- Loan approvals granted to uncreditworthy employees.
- Lack of independence between the approval and disbursement functions.
- Frequent sales of collateral (land flips) indicating related party transactions.
- Predatory lending practices.

### *Red Flags of Appraisal Abuse*

- No appraisal or property evaluation in file.
- One appraisal in file, but appraisers billed institution for more than one.
- Unusual appraisal fees (high or low).
- No history of property or prior sales records.
- Market data located away from subject property.
- Unsupported or unrealistic assumptions relating to capitalization rates, zoning change, utility availability, absorption, or rent level.
- Valued for highest and best use, which is different from current use.
- Appraisal method using retail value of one unit in condo complex multiplied by the number of units equals collateral value.
- Use of superlatives in appraisals.
- Made for borrower.

- Appraisals performed or dated after loan.
- Close relationship between appraiser, lender and/or borrower.

### *Red Flags of Check Fraud*

Check fraud is one of the largest challenges facing financial institutions. Forty-three percent of the Suspicious Activity Reports between April 1996 and September 1997 related to check fraud, counterfeit checks, and check kiting. A 1996 study by the Federal Reserve estimated financial institutions suffered losses of \$615.4 million involving 529.1 thousand cases in 1995. Savings associations accounted for \$67.5 million of the losses and 65.4 thousand of the cases. The Check Fraud Working Group, a subgroup of the Interagency Bank Fraud Working Group prepared a booklet in February 1999, *Check Fraud: A Guide to Avoiding Losses*. In the booklet, the Check Fraud Working Group identifies and discusses in detail the following check fraud schemes:

- Altered checks.
- Counterfeit checks.
- Forged checks.
- Checks drawn on closed accounts.
- Identity assumption.
- Fraud by bank insiders.
- Telemarketing fraud.
- Check fraud by gangs.

Savings associations can take the following preventive measures to reduce check fraud:

- Establish and maintain strong organizational controls.
- Ensure that effective internal controls are actively in place to prevent check fraud by insiders.
- Provide effective check fraud prevention programs through education and training for front-line personnel, managers, and operations personnel.
- Furnish a special section in teller manuals about check fraud that includes a detailed list of common warning signs.

- Establish guidelines for check cashing.
- Provide specialized training for new account representatives and establish guidelines for opening new accounts.

## Suspicious Activity Reports (SAR)

### *Filing Requirements*

Paragraph (d)(3) of OTS regulation § 563.180, Suspicious Activity Reports and Other Reports and Statements, requires savings associations<sup>2</sup> and their service corporations to report suspicious activities. They are to file SARs with the appropriate federal law enforcement agencies and the Department of Treasury by sending them to the Financial Crimes Enforcement Network (FinCEN) of the Department of the Treasury. The regulation requires a filing after the discovery of a known or suspected federal criminal violation that involves any of the following persons or transaction:

- Any officer, director, employee, agent, or other institution-affiliated person.
- Transaction(s) aggregating \$5,000 or more in funds or other assets, when there is a factual basis for identifying a suspect.
- Transaction(s) aggregating \$25,000 or more even though a suspect is unidentified.
- Transaction(s) aggregating \$5,000 or more that involve potential money laundering, or violations of the Bank Secrecy Act.

Section 563.180(d)(5) requires a savings association or service corporation to file an SAR no later than 30 calendar days after the date of initial detection. If there is no identified suspect on the date of detection, however, an association or service corporation may delay a filing up to an additional 30 days to identify a suspect. If a violation requires immediate attention, such as when it is ongoing, an association or service corporation must by telephone immediately notify an appropriate law enforcement authority and OTS. They must also file a timely SAR.

Section 563.180(d) also does the following:

- Encourages savings associations and their service corporations to file a copy of the SAR with state and local law enforcement agencies where appropriate.
- Provides that institutions need not file SARs for robberies and burglaries that they report to appropriate law enforcement authorities.

---

<sup>2</sup> Section 563.180(d) treats a savings association and its operating subsidiaries as one unit.

- Requires that institutions retain copies of SARs, and supporting documentation, for five years from the date they file them.
- Advises that failure to file a SAR in accordance with this section may subject the savings association, or service corporation, its officers, directors, employees, agents, or other institution-affiliated parties to supervisory action.
- Advises that the law shields financial institutions and their employees from civil liability when they report suspicious activities.

Financial Crimes Enforcement Network (FinCEN) inputs the information reported in SARs into a central database, which is accessible only to federal and state financial institution regulators and law enforcement agencies. The usefulness of the database depends on the completeness and accuracy of the reported information. Accordingly, you should ensure that associations are accurately and fully completing SARs.

### *Examiner and Regional Reporting Requirements*

Savings associations and their service corporations have the primary responsibility to file SARs. You must, however, complete and file a SAR when the required filing institution has either failed to do so or has not properly completed or filed it. When necessary, you should seek filing guidance from your supervisors or regional legal or enforcement personnel, including guidance concerning Right to Financial Privacy Act issues.

### USA PATRIOT Act of 2001

In October 2001, President George W. Bush signed anti-terrorism legislation that gives law enforcement authorities an array of new powers to use in the nation's campaign against terrorism. The new law, called The USA PATRIOT Act of 2001, contains sweeping new surveillance powers for law enforcement agencies, but some of these new powers will expire in four years.

The new law's money laundering provisions will accomplish the following:

- Bolster law enforcement's ability to find and destroy the financing of terrorist organizations, whether in banks or in underground "hawala" systems.
- Establish a government-industry partnership to stop terrorist funding in real-time.
- Track any terrorist money kept in secret offshore havens and increase foreign cooperation with U.S. efforts.
- Require banks to monitor certain accounts held by non-U.S. citizens.
- Give the government the power to require foreign banks to reveal customers transaction information under certain conditions.

- Make it a crime to smuggle currency in excess of \$10,000 and to knowingly falsify a customer's identity when making a transaction or opening an account with a financial institution.
- Create a highly secure Web site within the FinCEN, giving financial institutions the means to notify authorities quickly when a suspicious transaction takes place. Further measures would update counterfeiting laws to address technological advances used in the counterfeiting of U.S. currency.

You should be aware of the new law when examining institutions for fraud, internal control (especially wire transfers), or when reviewing SARs. If you have concerns or questions see the FFIEC BSA/AML Examination Manual.

### *Confidential Individual Information System*

In addition to contributing to and using the FinCEN database, OTS utilizes its own automated system, the Confidential Individual Information System (CIIS), to record information on individuals. The recorded information concerns the following types of events:

- Enforcement actions.
- Referrals to a professional organization for disciplinary reasons.
- Liability suits, investigations as to unusual transactions.
- Certain application activity (such as acquisition or change of control, and procurement of a charter).

Other federal agencies and state authorities may access CIIS information, with the approval of the OTS national administrator or a region's CIIS administrator.

### Regional Fraud and Insider Abuse Program

Each region must maintain a written fraud and insider abuse program, and should designate a person to be a Criminal Referral Coordinator to administer the program. The coordinator should act as a contact person or liaison to develop and maintain both internal and external fraud and insider abuse operations and communications.

While the extent of a regional program will be dependent on the incidences of fraud and insider abuse within the region, at a minimum each region (operations or legal) is responsible to do the following:

- Monitor and review regional SARs entered into the FinCEN system, particularly those that involve institution-affiliated persons or significant losses. As appropriate, communicate to the staff the reported suspicious activities.

- Ensure that institutions (and OTS staff, when necessary) complete and file accurate and timely SARs, including the providing of assistance and advice in such filings.
- Exchange information with and provide assistance to the FBI, Department of Justice, and other agencies, and ensure that appropriate persons follow up promptly on important SARs.
- Participate with local interagency bank fraud working groups that meet within the region.
- Ensure compliance with the Right to Financial Privacy Act as it relates to providing information and documentation to law enforcement and other government agencies.
- Work with OTS regional counsel office and OTS Enforcement Division in matters that relate to investigations for criminal prosecution or civil enforcement actions.
- Be able to provide background information reports on regional fraud and insider abuse cases, including prosecutions in progress and the outcome of important institution-affiliated person cases.

Regional directors are responsible to ensure that regional staff receives adequate training to accomplish the examination objectives and procedures set forth in this handbook section.

## REFERENCES

### United States Code (12 USC)

§ 3401 Right to Financial Privacy Act of 1978

### United States Code (18 USC)

§ 215 Kickbacks and Bribes

§ 657 Theft, Embezzlement, or Willful Misapplications of Funds

§ 709 False Advertising or Misuse of Names to Indicate Federal Agency

§ 1001 General False Statements

§ 1006 False Entries or Reports

§ 1014 False Statements

§ 1344 Bank Fraud

§ 1517 Obstructing Examination of Financial Institution

## Code of Federal Regulations (12 CFR)

Part 215	Regulation O, Loans to Executive Officers, Directors and Principal Shareholders of Member Banks
§ 561.14	Controlling Person
§ 561.18	Director
§ 561.24	Immediate Family
§ 561.35	Officer
§ 563.33	Directors, Officers, and Employees
§ 563.41	Loans and other Transactions with Affiliates and Subsidiaries
§ 563.43	Loans by Savings Associations to their Executive Officers, Directors and Principal Shareholders
§ 563.130	Prohibition on Loan Procurement Fees
§ 563.170(a)	Examinations and Audits
§ 563.180(d)	Suspicious Activity Reports
§ 563.200	Conflicts of Interest

## Office of Thrift Supervision Bulletins

RB 20	Proper Investigation of Applicants and Increased Communication Between OTS and other Financial Institution Regulatory Agencies
-------	--

## Interagency Guidance and Forms

*Check Fraud: A Guide to Avoiding Losses* (February 1999)

Suspicious Activity Report Form

## American Institute of Certified Public Accountants

Statement on Auditing Standards, No. 82, Consideration of Fraud in a Financial Statement Audit (February 1997) (AU 316)

The Auditor's Responsibility to Consider Fraud and Error in an Audit of Financial Statements – International Standards on Auditing (ISA No. 8240, Appendix 3)

**This page intentionally left blank**



# Fraud and Insider Abuse Program

---

## EXAMINATION OBJECTIVES

To recognize warning signs of fraud and insider abuse and to take appropriate measures to follow-up on possible instances of such activity.

To determine if the institution's internal control system is applicable to officers and directors as well as other employees.

To determine the institution's risk exposure associated with each significant instance of fraud or abuse.

To identify weaknesses in the institution's internal controls through detection and analysis of any patterns of fraud or abuse.

To properly report suspected criminal misconduct uncovered during the examination to appropriate law enforcement authorities.

To determine if the institution is reporting suspected criminal acts as § 563.180(d) requires.

To determine if the institution is properly completing SARs.

To determine if the institution has an adequate program of follow-up with law enforcement authorities regarding SARs it has filed.

## EXAMINATION PROCEDURES

### LEVEL I

WKP. REF

1. Review the adequacy of the institution's policies and procedures with respect to conflicts of interest. Determine whether the institution requires directors, officers, and employees to sign a Code of Ethics statement.

- 
2. Discuss the issue of fraud and insider abuse with the internal auditors and, if necessary, the external auditors to assess whether they have any concerns. Determine if they have made any reports on suspected fraud to the board or others.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Fraud and Insider Abuse Program

---

WKP. REF.

3. Review the results of the questionnaires to determine if adequate controls are in place to mitigate fraud. Assess the adequacy of controls that would prevent officers and directors from perpetrating fraud.
- 

4. Review the results of the various examination programs to determine if problems exist that may be symptomatic of fraud. In cases where fraud may be likely, investigate such problems to determine the cause of the problem (for example, poor staff training, errors, poor judgment).
- 

5. Review the institution's policies and procedures on reporting suspected criminal activity to law enforcement agencies and its board of directors for compliance with § 563.180(d).
- 

6. Review the institution's SARs, including those that OTS has filed, to determine if any patterns of criminality exist:

- Identify multiple SARs on individual suspects, location of violation (for example, loan center, savings branch), or type of violation.
  - Analyze any apparent pattern of fraud or abuse to determine if enhanced internal controls would deter any future abuse.
- 

7. Review all significant SARs, other reports, and patterns to determine if the institution has properly identified and addressed all related financial, operational, and legal risks; for example, valuation allowances established, internal controls strengthened, etc.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Fraud/and Insider Abuse Program

---

WKP. REF.

8. Assess the institution's risk of fraud by reviewing the red flag warning signals and conditions in the institution. You should do this in conjunction with performing other examination programs and procedures, completing the Fraud Risk Evaluation Form (Appendix A) and, if necessary, by other appropriate means. You should notify your supervisor when you have rated any individual fraud risk score 4 or 5, and you believe that there is significant potential for insider abuse or fraud.

---

9. Consult with other examination crewmembers concerning the need to expand examination scope within certain areas based on an indication of a higher than acceptable risk of fraud within certain areas of the institution.

---

10. Notify the regional legal staff if any person attempts to obstruct the examination, in possible violation of criminal statute 18 USC 1517.

---

11. Obtain a list of deposit and loan accounts of directors, officers, and other affiliated persons. Test check these accounts for preferential rates and, for deposit accounts, appropriate board approval of any overdrafts.

---

12. Review Level II procedures and perform those necessary to test, support, and present conclusions derived from performance of Level I procedures.

---

## LEVEL II

1. Choose a sample of SARs that the institution has filed. Review each sample SAR to determine its accuracy, completeness, timeliness, and propriety.

---

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Fraud and Insider Abuse Program

---

WKP. REF.

2. Complete the following procedures if you have identified any instance of suspected criminal misconduct:

- Immediately notify the EIC and field manager.
- Consult with appropriate regional office staff or counsel to determine a course of action, including preparation of a SAR.
- Obtain input from regional office legal staff on Right to Financial Privacy Act issues during the preparation of every SAR.

The following elements are particularly important in preparing a successful SAR:

- A chronology of events.
- A summary of suspected violations.
- A list of key participants or affiliates.
- A list of potential helpful witnesses.
- Any supporting documentation.

---

3. Review the institution's independent audit reports to determine if specific procedures exist to detect fraud, as the American Institute of Certified Public Accountants (AICPA) rules require.

---

4. Review the institution's program of follow-up with law enforcement authorities to determine if timely and adequate follow-up is being conducted on significant SARs.

---

5. For institutions with composite ratings of 4 or 5, determine if, in possible violation of 12 USC § 1828(k), the institution has done either of the following:

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Fraud/and Insider Abuse Program

---

WKP. REF.

- Made, or has entered into an agreement to make, any golden parachute or indemnification payments.
  - Prepaid any salary, or any liability or legal expense, in anticipation of insolvency and with a view towards preventing the proper use or purpose of assets.
  - Notify the regional legal staff if the institution has done either one.
- 

6. Ensure that your review meets the Objectives of this Handbook Section. State your findings and conclusions, and appropriate recommendations for any necessary corrective measures, on the appropriate work papers and report pages.
- 

## EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

**This page intentionally left blank**

### Fraud Risk Evaluation Form

Institution	Docket No.
Prepared by	Date
Reviewed by	Date

**Instructions**

This form documents your overall assessment of the level of fraud risk within the institution. Rate each risk factor from 1 to 5 with 1 indicating the lowest level of concern and 5 indicating the highest level of concern.

An individual factor rated 4 or 5 indicates that the institution is vulnerable to fraud. If fraud conditions or circumstances other than the factors listed below indicate a higher risk than normal, describe them on a separate sheet and attach it to this form. After you consider all relevant factors you should make an overall assessment of fraud risk and indicate its effect, if any, on the scope of the examination.

General Factors	Indicator		Comment or Description <sup>1</sup>	Risk Factor
	Lower	Higher		
Top management operating style	Effective board oversight	Domination of decisions by a single person		
Financial reporting	Conservative; accurate	Liberal; questionable; inaccurate		
Management turnover, including senior accounting personnel	Nominal	High		
Emphasis on meeting earnings projections	Little	Very high		
Profitability relative to industry	Adequate and consistent	Inadequate or inconsistent		
Growth within last three years	Stable	Rapid		
Financial condition	Healthy	Distressed		
Oversight of branches and subsidiaries	Centralized; strong oversight	Decentralized; weak oversight		
Indicators of going-concern problems	No serious indications of failure	Failure a distinct possibility		
Disagreements with auditors or examiners	None	Many		
Difficult-to-audit transactions or balances	Few	Many		
Misstatements detected in prior audits or examinations	Few and immaterial	Significant or material misstatements		
Examiner relationship with management	Cordial and constructive	Confrontations		
Response to supervision	Very responsive	Unresponsive		
Disclosures of director's and officer's outside interests	Fully disclosed	Not disclosed		
Background checks made on new directors, officers, and employees	Checked and verified	Not checked		
Internal auditor restrictions	None; auditor performs full scope reviews	Auditor works with restrictions, or on limited projects		
Internal auditor reporting	Reports to board or audit committee	Reports to management		
Internal audit department turnover	None or minimal	High		

General Factors	Indicator		Comment or Description	Risk Factor
	Lower	Higher		
<b>Policies and procedures</b>	Well developed for all areas of operations	None or poorly developed		
	Applied equally to employees and management	Not followed or circumvented by management or key employees		
<b>Unusual or lavish fixed assets</b>	None	Boats, aircraft, artwork, condos, etc.		
<b>Internal controls</b>	Sound system of controls	Material control deficiencies; or controls do not apply to top management		
<b>Response of management in providing documents to examiners</b>	Documents provided quickly	Long delays in getting documents		
<b>Transactions with other financial institutions</b>	Appropriate for business activities	Large transactions with small out of state banks		
<b>Board reports</b>	Accurate and complete	Inaccurate; inadequate; incomplete		
<b>Organizational structure</b>	Simple	Overly-complex		
<b>Aggressive accounting practices/tax-motivated behavior</b>	Few	Many		
<b>Regulatory violations</b>	Few	Many		
<b>Criminal Referrals</b>	Few	Many		
<b>Falsified bank records</b>	None	Many		

**Lending Factors**

<b>Loan documentation</b>	Well-documented loans and credit quality	Poorly documented loans		
<b>Loan performance tracking</b>	Close review of problem credits by management and the board	No (or erroneous) past due or watch list reports		
<b>Borrower financial statements</b>	Borrowers' financial position well documented	No (or unsigned) financial statements		
<b>Loan disbursements</b>	Well documented; approved by an independent officer	Questionable; approved by loan officer		
<b>Corporate loans</b>	Proper endorsements and guarantees	No (or inadequate) endorsements and guarantees		
<b>Resolution of problem loans</b>	Well documented and reasonable	Questionable pay-downs prior to examination or audit		
<b>Overdrafts</b>	Properly approved; reasonable amounts	Large questionable overdrafts		
<b>Refinancing</b>	Well documented; properly approved	Poorly documented; refinanced by a different department		
<b>Nominee loans</b>	No nominee loans	Nominee loans made		
<b>Loan terms</b>	Loan size, rates and maturities appropriate	Loans of unusual size, rates, and maturities		
<b>Evergreen/non-amortizing loans</b>	No evergreen/nonamortizing loans	Several large evergreen/nonamortizing loans		
<b>Real property sales history</b>	Well-documented history of sales and ownership	No history of sales or ownership		
<b>Out of territory loans</b>	No out of territory loans	Many out of territory loans		
<b>Brokered loans</b>	No brokered loans	Loans from brokers		
<b>Adequacy of collateral</b>	Loans adequately collateralized when appropriate	Large loans with unusual, questionable, or no collateral		
<b>Collateral sales history</b>	Collateral sales history is reasonable	Frequent sales; flipped collateral		
<b>Loans to directors, officers, and employees</b>	Properly underwritten and reported to the board of directors	Loans to uncreditworthy directors, officers, or employees		



Lending Factors	Indicator		Comment or Description	Risk Factor
	Lower	Higher		
<b>Lending authority</b>	Large approval limits are vested in the board or its committee	Large approval limits given to individuals or to inexperienced or inappropriate employees		
<b>Third-party disbursements</b>	Disbursements made to borrowers	Disbursements made to third parties		
<b>Construction disbursements</b>	Property inspected by independent institution officer prior to disbursement	No or poorly documented inspections; no rotation of inspectors		
<b>Asset performance</b>	Very low percentage of delinquent/nonperforming/classified assets	High percentage of delinquent/nonperforming/classified assets		
<b>Independent loan review function</b>	Effective; independent loan review function	No (or ineffective) loan review		
<b>Speculative, high-risk lending activities</b>	Institution has conservative lending practices	Institution engages in high-risk lending activities		
<b>Predatory lending practices</b>	None	Institution engages in predatory lending practices		

**Deposit Factors**

<b>Concentrations of deposits</b>	No concentrations of deposits	High concentration of deposits by individuals, firms, or public entities		
<b>Brokered deposits</b>	No brokered deposits	High level of brokered deposits		
<b>Training for all personnel on effective check fraud prevention</b>	Comprehensive training program for all personnel on check fraud prevention	No training on check fraud prevention		
<b>Check cashing guidelines</b>	Comprehensive check cashing guidelines	No check cashing guidelines		
<b>New accounts</b>	Comprehensive guidelines for opening new accounts	No guidelines for opening new accounts		
<b>Signature cards</b>	Signature cards secure, permanent, and updated	No control over signature cards		
<b>Account changes</b>	Account changes require identification and written requests	No controls over account changes		
<b>Dormant accounts</b>	Dormant account activity requires extra approvals or mandatory holds	No controls on dormant accounts		

<sup>1</sup> Required if factor is rated 4 or 5.

**We modified the examination scope in the following areas in consideration of the risk factors identified above:**

---



---



---



---

**This page intentionally left blank**

---

## Questions and Answers - Examination Obstruction

**Question: What should I do if an association tells me that the documents that I need are inaccessible because they are in remote storage off site?**

*Answer:* Advise the association that it must give you the documents' specific location and immediate and complete access to wherever the association stored the documents. 12 USC §1464(d)(1)(B)(ii) and 12 CFR § 563.170(c).

**Question: What should I do if an association refuses to provide me with access to any records until the OTS Director requests access, since 12 USC § 1464(d)(1)(B)(ii) uses the phrase, "upon request by the Director"?**

*Answer:* As an examiner appointed by the Director, you have the delegated authority to act on the Director's behalf in the examination of federally insured thrifts. 12 USC §§ 1462a(h)(4), 1463(a)(1) and 1464(a). Your request for records meets these statutory requirements; the association must provide you with prompt and complete access.

**Question: What should I do if an association asserts privilege and refuses to provide me with access to documents about a large, nonperforming commercial property loan because the borrower has sued the institution?**

*Answer:* Consult with your EIC, field manager, or regional counsel, as this is not a matter protected from regulatory review by an attorney-client privilege. The association must immediately instruct its counsel to provide you with prompt and complete access to all documents and records concerning the status of this loan. 12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 563.170(c).

**Question: What should I do if an association tells me it has no underwriting records on a large, real property loan?**

*Answer:* Advise the association that OTS will cite it for violation of 12 CFR §§ 560.100, 560.101, and/or 563.170(c), and proceed with a more thorough review of this asset. Remain alert to the possibility that the documents exist but are being withheld. Staff comments or documents in other files might indicate the missing association records were created. Like withholding documents, failure to create and maintain critical documents is a red flag indicating possible fraud, insider abuse, or financial manipulation. Keep your EIC or field manager apprised of your findings.

**Question: What should I do if I request documents during a focused, special limited examination and the association denies me access because it is not a regularly scheduled, full-scope examination?**

*Answer:* Federal law requires associations to provide examiners, including safety and soundness, compliance, trust, and information systems examiners, prompt and complete access to all association records and employees during any type of examination. The statute does not limit the authority to examinations of a specific length, scope, or type. 12 USC § 1464(d)(1)(B)(ii).

**Question: What should I do if I request accounting records on a particular transaction and the association's auditor denies me access based on an assertion of accountant-client privilege?**

*Answer:* There is no such generally recognized privilege. The auditor must provide you with prompt and complete access to the documents. Notify your regional counsel and regional accountant because this may be an ethical or contractual breach by the auditor.

**Question: What should I do if an association denies my request outside an examination for access to the documents necessary to perform a status update on a large, troubled loan?**

*Answer:* You are working to determine the condition of the association in the course of supervision. The association must give you prompt and complete access to all relevant documents and records of any type. 12 USC § 1464(d)(1)(B)(iii).

**Question: What should I do if an association tells me that I may review copies of loan files maintained by computer, but may not review originals because the originals are stored off site in a remote facility for safekeeping and cannot retrieve the originals without considerable expense.**

*Answer:* This is an impermissible screening tactic. As yet, you have no assurances that the copies are exactly the same as the originals or that the originals have all the required disclosures and signatures. You have no assurances that the originals ever existed, or still exist. Additionally, the association's computer may be tracking which documents you are retrieving, permitting the association to review and "correct" any problems with the originals before you see them. The association must provide you with prompt and complete access to all relevant documents of any type, especially originals, wherever those documents may be. 12 USC § 1464 (d)(1)(B)(ii) and 12 CFR § 563.170(c).

**Question: What should I do if an association's board of directors refuses to allow me to observe their meetings, citing reasons such as highly confidential merger discussions, personnel issues, or the like?**

*Answer:* 12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 563.170(c) obligate the association to allow you to attend the meetings. Additionally, you may remind the directors that 12 CFR § 510.5 prohibits you, as an examiner, from disclosing or permitting the disclosure of proprietary or confidential association information obtained through OTS examination and supervision functions.

**Question: What should I do if an association designates a particular employee to assist the examination team to find and locate documents, but that employee is frequently unavailable to assist?**

*Answer:* It may be appropriate for the association to designate an individual to assist the examination team, as long as the arrangement provides you with "prompt and complete" access to records and staff. You should insist upon access to information within a reasonable time. In some circumstances, a "reasonable" time may require immediate access to information. In all cases, because of examination schedules, the association must arrange to comply quickly with your information requests.

**Question: What should I do if an association requires that outside counsel review requested documents for privilege before producing them for my review, or that an attorney be present when I wish to interview an employee?**

*Answer:* In both cases, alert your EIC, field manager or regional counsel. In the first case, insist that counsel's review be conducted quickly and without unreasonably delaying your access to the documents. Insist upon access to the original documents and a written list of any requested documents withheld based on a claim of privilege. In the second case, requiring association counsel to be present is an impermissible restriction on your access to information. You should inform management that you would not agree to any such restrictive condition on your right to interview and obtain information from any officer, employee, or agent of the association.

**Question: What do I do if the thrift holding company is an insurance company regulated by a state Insurance Commissioner?**

*Answer:* Continue with your holding company exam as you normally would. (You may use information from, or provided to the state Insurance Commissioner. Regional offices should request this information in advance.) The Gramm-Leach-Bliley Act (GLBA) does not apply to holding companies or insured depository institutions themselves. Therefore, you may perform a full examination of the holding company. 12 USC §§ 1831v(c) and 1467a(b)(4).

**Question: What do I do if I discover extensive business records of a functionally regulated affiliate at the holding company, along with other records that I have access to?**

*Answer:* You may review any records maintained on holding company premises. Generally, the GLBA limits the circumstances under which you may go on the premises of a functionally regulated entity. The GLB also limits your ability to order documents or talk to the staff of a functionally regulated entity. The GLB does not prevent you from reviewing records maintained on holding company or thrift premises. 12 USC § 1831v(a).

**Question: What do I do if I determine, in the course of an examination, that an insurance subsidiary of a thrift holding company may pose a material risk to the safety and soundness of the association? The functionally regulated affiliate provides low premium, large limit coverage for high risk items (concentrations of hurricane coverage along the Southeast Atlantic) and places its portfolio in high risk investments (junk bonds)?**

*Answer:* You should have already reviewed the publicly available records, externally audited financial statements, information available at the holding company's premises, and any available state insurance commissioner's or regulator's examinations and other reports about the functionally regulated affiliate. You or your supervisor should have discussed your concerns with the commissioner's or regulator's office. Highlight the bases for your concerns in the documents available and discuss the information with your supervisor, regional counsel, and (possibly) the regional director. Together you will determine whether these facts warrant an on-site OTS examination of the functionally regulated affiliate. You should document your work paper files to indicate which of the GLBA criteria you base the justification for your examination. If there is the potential for enforcement action, such as the issuance of a subpoena, you should include regional enforcement counsel in your discussions.

**Question: What should I do if the association engages in transactions with an affiliate that is functionally regulated and all of the TWA records are on the functionally regulated affiliate's premises?**

*Answer:* We enforce the rules concerning the association's transactions with affiliates. Therefore, the association must provide you with "prompt and complete" access to all relevant documents and staff concerning any transaction involving the association wherever they may be, even if located on the premises of a functionally regulated affiliate. You may require an association to obtain and keep records necessary for it to oversee the transactions. 12 USC § 1464(d)(1)(B)(ii) and 12 CFR § 570(c). Your review of the association's TWA materials at their storage site does not constitute the examination of a functionally regulated affiliate under the GLBA. An association or a thrift holding company cannot shield its documents or transactions from your review by storing them at the offices of a functionally regulated affiliate.

**Question: What should I do if I need to interview a dual employee, a person who is employed both by the association and a functionally regulated affiliate?**

*Answer:* You may interview the employee concerning matters within the scope of his or her duties and responsibilities on behalf of the association.



## Transactions with Affiliates and Insiders

Affiliate relationships and transactions with insiders can significantly affect a savings association's operations and overall financial condition. Your review of these transactions is a critical component of savings association and holding company examinations. However, the rules on affiliate transactions and transactions with insiders are complex and, at times, confusing. This Section will give you a basic understanding of these rules. You should carefully review all such transactions to identify any potential risks they pose to the savings association and ultimately to the deposit insurance fund.

As competition among providers of financial services has increased, companies have pursued opportunities to enhance operating synergies among affiliated entities and to leverage expertise and resources throughout their overall organizational structure. Such relationships can present unique challenges for regulators, for example, in identifying the flow of funds among entities and assessing internal controls for oversight of savings association/affiliate arrangements.

---

### LINKS

-  [Program](#)
  -  [Appendix A](#)
- 

In many cases, it is appropriate and beneficial for an association to engage in business transactions with its affiliates and insiders. Statutes and OTS rules, however, may limit or prohibit these affiliate transactions. Additionally, OTS may prohibit any transaction when contrary to the association's best interests, based on safety and soundness grounds and even abuse. Accordingly, you must distinguish appropriate transactions from abusive or potentially abusive transactions, or transactions that are otherwise inconsistent with safe and sound operations.

The association's affiliate transactions should meet the following criteria:

- Not be abusive or detrimental to the savings association. (You should be alert to any transaction that subjects the association to unreasonable pressure from management or an affiliate.)
- Be based on safe and sound practices.
- Comply with applicable statutory and regulatory standards. You may find OTS transactions with affiliates rules at 12 CFR § 563.41. Restrictions on transactions with insiders (i.e., association or affiliate directors, executive officers, principal shareholders, and related interests) are at 12 CFR § 563.43.

This Section should help you evaluate the following areas:

- Acceptability of transactions with affiliates.

- Permissibility of transactions with insiders.

## TRANSACTIONS WITH AFFILIATES

Affiliate transactions occur when an association engages in a transaction with its holding company, a subsidiary of the holding company, any other affiliate or, under certain circumstances, an unrelated third person. You may find evidence of such transactions at any association, but the volume of affiliate transactions is usually greater in a holding company structure since inter-company transactions are often an integral part of a company's operations.

Due to the potential risk from these transactions, associations are subject to the following regulatory standards:

- Individual and aggregate ceilings on the dollar amount of affiliate transactions. These ceilings are based on a percentage of capital and surplus.
- Arms-length dealings requirement.
- Prohibition of acquisitions of low-quality assets from affiliates.
- Collateralization requirements for affiliate credit transactions.
- Prohibition of certain activities.

## Compliance with Statutory and Regulatory Standards

Section 11 of the Home Owners' Loan Act (HOLA) applies §§ 23A and 23B of the Federal Reserve Act (FRA) to savings associations "in the same manner and to the same extent" as if the association were a member bank. Section 11 also applies two additional prohibitions to associations. Specifically, § 11 prohibits associations from purchasing or investing in securities issued by affiliates (other than with respect to shares of a subsidiary), and from making loans or extensions of credit to affiliates engaged in non-bank holding company activities.

The Board of Governors of the Federal Reserve System's (FRB) Regulation W (12 CFR Part 223) implements §§ 23A and 23B of the FRA for member banks. The OTS rule (12 CFR § 563.41) requires savings associations to comply with Regulation W as if they were member banks, interprets Regulation W to apply it to savings associations, and implements the additional restrictions in § 11 of the HOLA.

The intent of 23A and 23B is to protect against a depository institution suffering losses in transactions with affiliates and to limit the ability of a depository institution to transfer to its affiliates the subsidy arising from the institution's access to the federal safety net.



---

## Compliance with § 23A of the FRA and the additional prohibitions under § 11 of the HOLA

You should consider the following questions when you determine whether a particular transaction complies with § 23A of the FRA and the two additional prohibitions under § 11 of the HOLA. We discuss compliance with § 23B of the FRA later in this Handbook Section.

- Is the transaction with an affiliate?
- Is the transaction a covered transaction?
- Is the transaction exempt?
- Does the covered transaction meet the quantitative restrictions?
- Does the transaction meet the qualitative restrictions (including collateral requirements, if it is a loan)?

We will review each of these considerations in the following pages.

### *Is the Transaction with an Affiliate?*

As a first step, you must identify all of the association's affiliates.

Affiliates. Generally, affiliates include the following companies. (*Note*: individuals are not “affiliates” for the purposes of the transaction with affiliates restrictions.)

- *Parent companies*. Any company that controls the savings association.
- *Companies under common control by a parent company*. Any company that is controlled by a company that controls the association.
- *Companies under other common control*. Any company controlled, directly or indirectly, by trust or otherwise, by or for the benefit of shareholders who beneficially or otherwise control, directly or indirectly, by trust or otherwise, the savings association or any company that controls the savings association. For example, if an individual (that is, not a company) controls an association and another company, that company would be an affiliate.
- *Companies with interlocking directorates*. Any company in which a majority of directors, trustees, or general partners (or individuals exercising similar functions) constitute a majority of the persons holding any such office with the savings association or any company that controls the savings association.

- *Sponsored or advised companies.* Any company, including a real estate investment trust, that the savings association or any affiliate sponsors and advises on a contractual basis.
- *Investment companies.* Any investment company for which a savings association or any affiliate serves as an investment advisor as defined in the Investment Company Act of 1940 (15 USC 80a-2(a)(20); or any unregistered investment fund for which a savings association or any affiliate serves as an investment advisor, if the savings association and its affiliates own or control in the aggregate more than five percent of any class of voting securities or of the equity capital of the fund.
- *Certain subsidiaries of savings associations.* Subsidiaries are discussed below.
- *Companies held under merchant banking or insurance company investment authority.* Any company in which the savings association's holding company owns or controls, directly or indirectly, or acting through one or more persons 15 percent or more of the equity capital under the merchant banking or insurance company investment authority at section 4(k)(4)(H) or (I) of the Bank Holding Company Act. This category is subject to several safe harbors and has a limited applicability to most associations. It applies only if the association is controlled by a holding company that was not a savings and loan holding company (or did not have a savings and loan holding company application in process) before May 4, 1999.
- *Partnerships.* Any partnership, if the association or an affiliate serves as a general partner or causes any director, officer, or employee of the association or affiliate to serve as a general partner.
- *Subsidiaries of affiliates.*
- *Other companies identified by OTS.* Any company that OTS determines, by regulation or order:
  - To have a relationship with the savings association, or any affiliate of the savings association, such that covered transactions by the savings association with that company may be affected by the relationship to the detriment of the savings association; or
  - To present a risk to the safety or soundness of the savings association.

Subsidiaries generally are not affiliates, and are considered equivalent to the association.

Subsidiaries. Subsidiaries (i.e., companies that are controlled by a savings association) generally are not affiliates, and are considered equivalent to the association. As a result, transactions between an association and its subsidiaries are generally not subject to the transactions with affiliate restrictions. At the same time, any affiliate of the savings association is also an affiliate of these savings association subsidiaries. A transaction between these subsidiaries and the association's affiliates are subject to affiliate restrictions.

---

Certain subsidiaries of a savings association, however, are affiliates. Subsidiaries that are affiliates include:

- *An insured depository institution that is a subsidiary of the savings association.* Please note however, that several exemptions including the sister bank/savings association exemption, limit the application of the affiliates rules to transactions with these associations.
- *A company that is also directly controlled by one or more affiliates* (other than an insured depository institution affiliate) of the savings association. For example, if an association owns 50 percent of the voting shares of its subsidiary and its holding company owns the remaining shares, the subsidiary would be treated as an affiliate.
- *A company that is also directly controlled by a shareholder* (or a group of shareholders) that also controls the association.
- *An employee stock option plan, trust, or similar organization* that exists for the benefit of the shareholders, partners, members, or employees of the savings association or any of its affiliates.
- *Any subsidiary that OTS determines to be an affiliate.*

You should be aware that Regulation W states that “financial subsidiaries” of member banks are affiliates. (See 12 CFR § 223.3(p) for a definition of this term.) OTS determined that savings associations do not have financial subsidiaries.

### Control.

A fundamental concept underlying the definition of affiliate is “control.” For the purposes of the affiliates restrictions, a company or shareholder has control over another company if:

- The company or shareholder, directly or indirectly, or by acting through one or more other persons, owns, controls, or has the power to vote, 25 percent or more of any class of voting securities of the other company.
- The company or shareholder owns or controls 25 percent or more of the equity capital of the other company, unless the company or shareholder demonstrates to OTS that it does not control the other company.
- The company or shareholder controls in any manner the election of the majority of the directors, trustees, or general partners (or individuals exercising similar functions).
- The OTS determines, after notice and opportunity for a hearing, that the company or shareholder, directly or indirectly, exercises a controlling influence over the management or policies of the other company.

In determining whether a company controls another, you should apply the following rules:

- A company controls securities, assets, or other ownership interests that are owned or controlled, directly or indirectly, by any subsidiary of the company.
- A company does not control another company by virtue of its ownership or control of shares in a fiduciary capacity, except as provided in the “companies under other common control” description above, or if the company owning or controlling shares is a business trust.
- A company or shareholder controls securities if it owns or controls instruments (including options or warrants) that are convertible or exercisable into the securities at the option of the holder or owner, unless the company or shareholder demonstrates to OTS that it does not control the security.

Please note that OTS used to apply the definitions and rebuttable presumptions of control in 12 CFR Part 574 to affiliate transactions. In 2003, OTS revised the affiliates rules to incorporate the concepts described above, and to delete references to Part 574. The scope of “control” may be broader or narrower under revised rule depending on the circumstances. If you have any questions, you should contact your regional counsel.

Companies that are not considered to be affiliates. Notwithstanding the definitions of affiliate discussed above, a company is not an affiliate if it meets any of the following criteria:

- The company engages solely in holding the premises of the savings association.
- The company engages solely in conducting a safe deposit business.
- The company engages solely in holding certain United State government securities.
- Control of the company is the result of the exercise of rights resulting from a bona fide debt previously contracted. Such entities, however, are not considered to be affiliates only for a limited period of time.

Transactions with third parties. A transaction between an association and any person will be treated as a transaction with an affiliate if the proceeds of the transaction are used for the benefit of, or transferred to, an affiliate. Under this “third party attribution rule,” for example, a loan to an unaffiliated third party will be attributed to an affiliate if the individual uses the funds to purchase an asset from an affiliate.

A transaction between an association and a third party will be treated as a transaction with an affiliate if the proceeds of the transaction are used for the benefit of, or transferred to, an affiliate.

Certain third party transactions are exempt from most § 23A restrictions. For example, if a third party uses a general purpose credit card issued by an association to purchase products and services from an affiliate, the association does not have to attribute the loan to the affiliate. To be a general purpose credit card, a

credit card must be widely accepted for the purchases of products and services by merchants that are not affiliates, and purchases from affiliates must be less than 25 percent of the total value of products and services purchased with the card by all cardholders (12 CFR § 223.16(c)(4)). These transactions are subject to safety and soundness requirements under § 23A and market terms requirements under § 23B.

Subject to certain conditions, OTS also does not apply the third-party attribution rule to the following transactions:

- Extensions of credit used to purchase assets through an affiliate that acts exclusively as an agent or broker in the transaction.
- Extensions of credit used to purchase securities through a security affiliate (that is, a registered broker-dealer) that acts exclusively as a riskless principal in the transaction.
- Brokerage commissions, agency fees, and riskless principal mark-ups in connection with these agency and riskless principal transactions.
- Preexisting lines of credit used to purchase securities from or through securities affiliates.

These transactions are subject to various conditions that are more fully described at 12 CFR § 223.16(b) and (c).

### *Is the Transaction a "Covered Transaction?"*

Once you determine that a transaction is with an affiliate, you must determine if it is a covered transaction.

Transactions that are subject to § 23A restrictions. If you answer "yes" to any of the following questions, the transaction is a covered transaction and is subject to the standards in § 23A.

*Has the association made a loan or extension of credit to an affiliate?* This category includes making or renewing a loan, granting a line of credit, or extending credit in any manner. Loans or extensions of credit include:

- Intraday credit.
- Leases that are the functional equivalent of a loan.
- Advances via an overdraft, cash item, or otherwise.
- The sale of Federal funds to an affiliate.
- The acquisition of a note or other obligation of an affiliate.

- An increase in the amount, extension of maturity, or adjustment to material terms of an extension of credit.
- Other similar transactions.

Certain less-obvious transactions may also constitute the equivalent of extensions of credit or other types of covered transactions. For example, intercompany payable/ receivable transactions, rent subsidies, and use of the association's personnel, premises, funds, or equipment without adequate compensation. Generally, if the association conducts such transactions on an arms-length basis, consistent with how they conduct transactions with a nonaffiliated party, OTS does not consider transactions "de facto" extensions of credit or covered transactions. However, you should review all such transactions to determine whether § 23A applies and, if so, whether the association complies with the applicable restrictions. You should also review the transactions for general safety and soundness concerns regardless of whether they are considered extensions of credit.

*Has the association purchased assets, including assets subject to recourse or a repurchase agreement, from an affiliate? A purchase of assets means an acquisition of an asset in exchange for cash or any other consideration, including an assumption of liabilities. The merger of an affiliate into a savings association is a purchase of assets if the association assumes any liabilities of the affiliate, or pays any other form of consideration in the transaction.*

*Has the association accepted securities issued by an affiliate as collateral security for a loan or extension of credit to any person or company? Securities include, for example, stocks, bonds, debentures, notes, or similar obligations (including commercial paper).*

*Has the association issued a guarantee, acceptance, or letter of credit on behalf of an affiliate? This category includes, for example, an endorsement or standby letter of credit on behalf of an affiliate, a confirmation of a letter of credit issued by an affiliate, and a cross-affiliate netting agreement. The category also includes credit derivatives that are the functional equivalent of a guarantee, such as credit derivatives between an association and a nonaffiliate in which the association protects the nonaffiliate from a default on, or decline in value of, an obligation of an affiliate.<sup>1</sup>*

Please note that the definition of covered transaction under Regulation W also includes the purchase of, or investment in, securities issued by an affiliate. Section 11 of HOLA generally prohibits these transactions for savings associations. See the following discussion.

**Prohibited Transactions.** For savings associations, § 11 of the HOLA prohibits two types of covered transactions. If you answer "yes" to either of the following questions, the transaction is prohibited.

---

<sup>1</sup> FRB has not yet determined whether other types of derivatives are covered transactions. If an association engages in such transactions with affiliates, however, it must establish policies and procedures to manage the credit exposures in a safe and sound manner. At a minimum, the policies and procedures must provide for monitoring and controlling the credit exposure (including imposing appropriate credit limits, mark to market requirements, and collateral requirements), and must ensure that derivative transactions with affiliates comply with the market terms requirements of § 23B. See 12 CFR § 223.33.

*Has the association purchased or invested in securities issued by any affiliate, other than shares of a subsidiary? For the purposes of this prohibition, a subsidiary includes a bank or savings association.*

*Has the association made a loan or extension of credit to an affiliate that is engaged in any activity that is impermissible for a bank holding company?*

OTS does not generally apply the third-party attribution rule to the § 11 loan prohibition. Thus, we will not prohibit a loan to a third party merely because proceeds are used for the benefit of, or transferred to, an affiliate that is engaged in nonbank holding company activities. However, if you determine that a loan to a third party is a prearranged step in a series of transactions designed to channel funds to such an affiliate, or is otherwise designed to circumvent the loan prohibition, you may inform the association that the transaction is, in substance, a prohibited loan. You may direct the association to divest the loan, unwind the transaction, or take other appropriate action.

Please note that OTS revised some long-standing interpretations of the § 11 loan prohibition in 2003. For example, OTS used to treat certain repurchase agreements as prohibited loans. OTS now treats repurchase agreements as asset purchases. While these transactions are no longer prohibited, they remain subject to §§ 23A and 23B restrictions. OTS also used to attribute activities of subsidiary companies to certain parent companies in determining whether the parent is engaged in impermissible bank holding company activities. OTS no longer attributes activities among affiliates.

OTS used to treat repurchase agreements as prohibited loans; we now treat them as asset purchases.

### *Is the Transaction Exempt?*

Regulation W exempts certain covered transactions from affiliate restrictions under § 23A. Pay particular attention to the scope of each exemption. All of the exemptions, for example, relieve associations from complying with the quantitative limits and applicable collateral requirements. All covered transactions remain subject to the safety and soundness requirements. Depending on the exemption, however, the low-quality asset purchase restriction may or may not apply. Exemptions from the market terms requirements under § 23B also vary and are discussed separately below.

The following transactions are exempt from the 10 and 20 percent quantitative limits on transactions with affiliates and the collateral requirements. These transactions are subject to safety and soundness requirements and prohibitions on purchases of low-quality assets:

- *Sister Bank/Savings Association Exemption.* Transactions with an insured depository institution if:
  - The savings association controls at least 80 percent of the voting securities of the depository institution;
  - The depository institution controls at least 80 percent of the voting securities of the savings association; or

- 
- A company controls at least 80 percent of the voting securities of both institutions (12 CFR § 223.41(a) and (b)).
  - *Purchases of nonrecourse loans from affiliated depository institutions.* This exemption applies to all affiliated insured depository institutions, including those that do not meet the 80 percent ownership requirement for the sister bank/savings association exemption (12 CFR § 223.41(c)).
  - *Internal corporate reorganizations.* Purchasing assets from an affiliate where the transaction is a part of an internal corporate reorganization of a holding company and involves the transfer of all, or substantially all, of the shares or assets of an affiliate or a division or department of an affiliate. This exception is subject to various requirements, including a prior written notice to OTS and a limitation on the amount of the transaction (12 CFR § 223.41(d)).<sup>2</sup>

The following transactions are exempt from the 10 and 20 percent quantitative limits on transactions with affiliates, collateral requirements, and the low quality asset purchase prohibition. These transactions are subject to safety and soundness requirements and to other requirements contained in the cited references to Regulation W:

- *Correspondent banking.* Making a deposit in an affiliated insured depository institution (or an affiliated foreign bank) that represents an ongoing working balance maintained in the ordinary course of correspondent business (12 CFR § 223.42(a)).
- *Uncollected items.* Giving immediate credit to an affiliate for uncollected items received in the ordinary course of business (12 CFR § 223.42(b)).
- *Credit transaction secured by deposits or U.S. government securities.* Engaging in a credit transaction with an affiliate to the extent that the transaction is and remains secured by any of the following:
  - Obligations of the United States or its agencies.
  - Obligations fully guaranteed as to principal and interest by the United States or its agencies.
  - A segregated, earmarked deposit account with the savings association that is for the sole purpose of securing credit transactions between the savings association and its affiliates, and is identified as such.

---

<sup>2</sup> A related provision exempts mergers and acquisitions that are step transactions. In step transactions, the association ultimately intends to acquire the company, but for various reasons, another affiliate acquires the company before transferring to the association. To qualify for the related exemption, the transaction must satisfy 12 CFR § 223.31(d). Unlike the internal corporate reorganization exemption, a step transaction is not subject to the prohibition on the purchase of low-quality assets.



---

If a loan is partially secured by collateral identified above, the portion of the loan that is secured by the collateral is exempt. The amount beyond the collateral's value is not exempt (12 CFR § 223.42(c)).

- *Purchase of securities of a servicing affiliate.* Purchasing securities of any company that is engaged solely in providing specified services, such as holding property used by the association, processing data, providing personnel services, performing accounting and auditing activities, and handling advertising and public relations (12 CFR § 223.42(d)).
- *Purchase of certain liquid assets.* Purchasing an asset having a readily identifiable and publicly available market quotation if the asset is purchased at (or below) that market quotation. An asset has a readily identifiable and publicly available market quotation if the asset's price is quoted routinely in a widely disseminated publication that is readily available to the general public, such as the Wall Street Journal (12 CFR § 223.42(e)).
- *Purchase of certain marketable securities.* Purchasing marketable securities from a securities affiliate (i.e., a registered broker-dealer). Among other requirements, the security must have a "ready market," may not be a low-quality asset, and must be eligible for purchase by a state member bank. Additionally, the purchase may not occur during or within 30 days of an underwriting if an affiliate is the underwriter, and the security's price must be electronically quoted in real-time by an unaffiliated quotation system (12 CFR § 223.42(f)).
- *Purchase of municipal securities.* Purchasing municipal securities from a securities affiliate (i.e., a registered broker-dealer). Among other requirements, the security must have a rating if the issuance does not exceed \$25 million and must be eligible for purchase by a state member bank. In addition, the securities price must be electronically quoted in real-time by an unaffiliated quotation system, verified by reference to two or more actual, current price quotes from unaffiliated broker-dealers, or verified by reference to a written summary provided by the syndicate manager to syndicate members (12 CFR § 223.42(g)).
- *Purchase of an extension of credit subject to a repurchase agreement.* Purchasing an extension of credit from an affiliate that the savings association originated and sold to the affiliate subject to a repurchase agreement or with recourse (12 CFR § 223.42(h)).
- *Purchase of assets by a newly formed savings association.* Purchasing an asset from an affiliate, if OTS approved the asset purchase in connection with its review of the formation of the savings association (12 CFR § 223.42(i)).
- *Transactions approved under the Bank Merger Act.* Mergers or consolidations between a savings association and an affiliated insured depository institution (or U.S. branch or agency of a foreign bank), and acquisitions of assets or assumptions of deposit liabilities by a savings association from such entities, if the transaction was approved under the Bank Merger Act (12 CFR § 223.42(j)).

- 
- *Purchases of extensions of credit.* Purchasing an extension of credit from an affiliate, on a nonrecourse basis, if all of the following requirements are met:
    - The affiliate must originate the extension of credit.
    - The association must perform its own independent evaluation of the creditworthiness of the borrower before the affiliate makes or commits to make the extension of credit.
    - The association must commit to purchase the extension of credit before the affiliate makes or commits to make the extension of credit.
    - The association may not make a blanket advance commitment to purchase extensions of credit from the affiliate.
    - The association may not purchase more than 50 percent of the total dollar amount of the extensions of credit originated by the affiliate, calculated on a rolling 12-month basis. OTS may impose a lower percentage (12 CFR § 223.42(j)).

This exemption was formerly codified at 12 CFR § 250.250. As a result, it is commonly referred to as the “250.250 exemption.”

- *Intraday extensions of credit.* Making intraday extensions of credit to an affiliate. An intraday extension of credit is a loan that the association expects to be repaid, sold, terminated, or fall within another exemption by the end of the business day. To qualify for this exemption, the savings association must comply with all of the following:
  - Establish and maintain policies and procedures reasonably designed to manage the credit exposure arising from the intraday extensions of credit to affiliates in a safe and sound manner, and to ensure compliance with market terms requirements at § 23B.
  - Have no reason to believe that the affiliate will have difficulty in repaying the extension of credit in accordance with its terms.
  - Cease to treat the extension of credit as intraday at the end of the association’s business day (12 CFR § 223.42(l)).
- *Riskless principal transactions.* Purchasing a security from a securities affiliate (i.e., a registered broker-dealer) if the association or the securities affiliate is acting exclusively as a riskless principal in the transaction, and the security is not issued, underwritten, or sold as principal (other than as riskless principal) by any affiliate of the association (12 CFR § 223.42(m)).

*Does the Covered Transaction Meet Quantitative Restrictions?*

Covered transactions with an affiliate are subject to quantitative restrictions. Through a review of internal records, you should verify that the association's aggregate amount of covered transactions is within both of the following quantitative limits:

- 10 percent of the association's capital stock and surplus with any single affiliate. An association may not enter into a covered transaction with the affiliate if the association would exceed this limit. You should be aware that OTS used to require associations to include all covered transactions with an affiliate's subsidiaries in determining the amount of covered transactions for the affiliate. OTS no longer requires this attribution.
- 20 percent of the association's capital stock and surplus with all affiliates. An association may not enter into a covered transaction with any affiliate if the association would exceed this limit.

Capital stock and surplus means unimpaired capital and unimpaired surplus as defined in the LTOB rule at 12 CFR § 560.93(b)(11).

In calculating compliance with the quantitative limits, you should attribute covered transactions with third parties to an affiliate to the extent that proceeds are used for the benefit of, or transferred to, the affiliate. You should also refer to the valuation and timing principles at 12 CFR § 223.21 (credit transactions); § 223.22 (asset purchases); § 223.24 (extensions of credit secured by affiliate securities); and § 223.31 (acquisitions of affiliates that become nonaffiliated subsidiaries after the acquisition).

*Does the Covered Transaction Meet Qualitative Restrictions?*

Covered transactions are also subject to various qualitative restrictions including a prohibition against purchases of low-quality assets; collateral requirements for credit transactions; and a general safety and soundness requirement.

Low-quality asset purchases. An association may not purchase a low-quality asset from an affiliate, unless the association made an independent credit evaluation and committed itself to purchase the asset before the affiliate acquired the asset. An association, however, may renew a loan participation involving certain problem loans if the transaction meets the requirements at 12 CFR § 223.15(b).

A savings association may not purchase a low-quality asset from an affiliate, unless the association made an independent credit decision to purchase the asset before the affiliate acquired the asset.

A low-quality asset includes:

- An asset (including a security) that is classified as substandard, doubtful, loss, special mention, or other transfer risk problems in the most recent report of examination or inspection prepared by a federal or state supervisor, or in any internal classification system used by the association or its affiliate.

- An asset in a nonaccrual status.
- An asset on which principal or interest payments are more than 30 days past due.
- An asset with renegotiated or compromised terms due to the deteriorating financial condition of the obligor.
- An asset acquired through foreclosure, repossession, or in satisfaction of a debt previously contracted, if the asset has not yet been reviewed in an examination or inspection.

Collateralization. A savings association must ensure that all credit transactions with affiliates are adequately collateralized.

The following types of transactions must be adequately collateralized: a loan, an extension of credit, the issuance of a guarantee, acceptance or letter of credit (including an endorsement or standby letter of credit on behalf of an affiliate and a confirmation of a letter of credit issued by an affiliate) and a cross-affiliate netting arrangement.

The collateral requirements do not apply to any of the following:

- Acceptances that are already fully secured by attached documents or by other property that is involved in the transaction and has an ascertainable market value.
- Unused portions of extensions of credit to an affiliate if the association has no legal obligation to advance additional funds until the affiliate provides the required collateral.

The collateral must have a market value equal at least equal to one of the following:

- *100 percent of the amount of the transaction* if the collateral consists of:
  - Obligations of the United States or its agencies.
  - Obligations fully guaranteed by the United States or its agencies as to principal and interest.
  - Notes, drafts, bills of exchange, or bankers' acceptances that are eligible for rediscount or purchase by a Federal Reserve Bank.
  - A segregated, earmarked deposit account with the savings association. The segregated, earmarked deposit must be for the sole purpose of securing credit transactions between the association and its affiliates and must be identified as such.
- *110 percent of the amount of the transaction* if the collateral consists of obligations of any State or political subdivision of any State.

- *120 percent of the amount of the transaction* if the collateral consists of other debt instruments, including loans and other receivables.
- *130 percent of the amount of the transaction* if the collateral consists of stock, leases, or other real or personal property.

The following assets are not acceptable collateral:

- Low-quality assets (defined above).
- Securities issued by an affiliate.
- Equity securities issued by the association.
- Debt securities issued by the association that represent the association's regulatory capital.
- Intangible assets, including servicing assets (unless specifically approved by FRB).
- Guarantees, letters of credit, and other similar instruments.

If the association does not maintain a first priority security interest in the collateral, it will be required to make certain deductions from the value of the collateral.

The association must maintain a security interest in the collateral that is perfected and enforceable under applicable law, including in the event of default resulting from bankruptcy, insolvency, liquidation, or similar circumstances. If the association does not maintain a first priority security interest in the collateral, it will be required to make certain deductions from the value of the collateral (12 CFR § 223.14(d)).

You should verify compliance with these collateral requirements through a review of the credit transaction and the types and levels of collateral established and maintained. The affiliate must replace collateral that is subsequently retired or amortized with additional eligible collateral where needed. This keeps the percentage of the collateral value relative to the amount of the outstanding credit transaction equal to the minimum percentage required at the beginning of the transaction.

Safety and soundness. An association may not engage in a covered transaction, including transactions that are exempt, unless the transaction is on terms and conditions that are consistent with safe and sound banking practices.

### Compliance with § 23B

In addition to a review of affiliate transactions to determine compliance with § 23A of the FRA and § 11 of the HOLA, you must determine whether transactions comply with § 23B of the FRA. Section 23B imposes market terms requirements on various covered transactions and prohibits certain other transactions.

### *Market Terms Requirement*

Covered transactions must take place on terms and under circumstances, including credit standards, that are substantially the same, or at least as favorable to the association, as those prevailing at the time for comparable transactions with nonaffiliates. In the absence of comparable transactions, the transaction must be on terms and under circumstances that, in good faith, would be offered to, or would apply to, nonaffiliates. In applying the market terms test:

- Is the transaction with an affiliate?
- Is it a covered transaction?

### Is the Transaction with an Affiliate?

Sections 23A and 23B use similar definitions of affiliate, with one exception. Under § 23B, affiliate excludes any insured depository institution. Please note that this exclusion is broader than the sister bank/savings association exemption under § 23A because there is no percentage-of-ownership test. Therefore, it is possible that a transaction between a savings association and an affiliated bank or savings association may be covered under § 23A because the 80 percent ownership criteria for the sister bank/ savings association exemption is not met. However, the transaction would not be subject to § 23B.

Like § 23A, § 23B has a third-party attribution rule. As a result, you must treat a transaction with a third party as a transaction with an affiliate if the proceeds from the transaction are used for the benefit of, or transferred to, the affiliate.

### Is the Transaction a Covered Transaction?

A covered transaction under § 23B is broadly defined to include the following transactions:

- A covered transaction under § 23A. Certain transactions that are exempt under § 23A are also exempt under § 23B. These include the exemptions for credit for uncollected items, credit transactions secured by deposits or U.S. government securities, purchases of securities of a servicing affiliate, purchases of certain liquid assets, purchases of an extension of credit subject to a repurchase agreement, asset purchases by a newly formed savings associations, and transactions approved under the Bank Merger Act. See 12 CFR § 223.52.
- A sale of securities or other assets to the affiliate, including assets subject to a repurchase agreement.
- A payment of funds or the furnishing of services to the affiliate under contract, lease or otherwise.
- A transaction in which an affiliate acts as an agent or broker or the affiliate receives a fee for its services to the association or any other person.

- A transaction with a third party when the affiliate has a financial interest, or is a participant, in the transaction or a series of transactions.

## *Prohibited Transactions*

Section § 23B prohibits the following transactions:

### Purchases as fiduciary

An association may not purchase, as fiduciary, any securities or other assets from any affiliate unless the purchase is permitted under the instrument creating the fiduciary relationship, by court order, or by law of the jurisdiction governing the fiduciary relationship.

### Purchases of securities underwritten by an affiliate

An association may not knowingly purchase or acquire a security, as principal or fiduciary, during the existence of any underwriting or selling syndicate where an affiliate is a principal underwriter of the security.

This prohibition does not apply if a majority of the association's directors:

- Approves the acquisition or purchase before the security is initially offered for sale to the public. The directors must base their approval on their determination that the purchase is a sound investment for the association, or for the person on whose behalf the association is acting as fiduciary; or
- Approves standards for acquisitions of such securities based on the determination that purchases under the standards would fulfill the sound investment requirement. Each acquisition must meet the standards. A majority of the directors must periodically review the standards to ensure they meet the sound investment requirement and review acquisitions to ensure that they meet the standards.

### Advertisements

Generally, an association and its affiliates may not publish any advertisement or enter into any agreement stating or suggesting that the association will in any way be responsible for the obligations of its affiliates. Nonetheless, an association may issue a guarantee, acceptance, or letter of credit on behalf of an affiliate, confirm a letter of credit issue by an affiliate, or enter into a cross-affiliate netting arrangement, if the transaction is otherwise permissible under § 23A. Since the association may enter into these transactions, it may also describe these transactions in disclosure documents if required by other laws.

### Compliance with Recordkeeping Requirements

An association must make and retain records that reflect, in reasonable detail, all transactions with its affiliates or with any other person to the extent that the proceeds of the transaction are used for the benefit of, or transferred to, an affiliate.

At a minimum, the records must:

- Identify the affiliate.
- Indicate the dollar amount of the transaction and show that the amount is within the applicable quantitative limitations specified in § 23A, or that the transaction is not subject to those limitations.
- Indicate whether the transaction involves a low-quality asset.
- Identify the type and amount of any collateral involved in the transaction and show that the collateral complies with the collateral requirements in § 23A, or demonstrate that the transaction is not subject to the collateral requirements.
- Demonstrate that the terms and circumstances of the transaction comply with the standards in § 23B, or that the transaction is not subject to those requirements.
- Show that loans and extensions of credit to affiliates are only made to affiliates that engage solely in activities permissible for bank holding companies.
- Be readily accessible for examination and other supervisory purposes.

### Compliance with Notice Requirements

OTS may require a savings association to notify the agency before it engages in transactions with affiliates (other than exempt transactions) or its subsidiaries. OTS may impose this notice requirement if:

- The savings association is in troubled condition. (That is, the savings association has a composite CAMELS rating of 4 or 5; is the subject of a capital directive, a cease and desist order, a consent order, a formal written agreement, or a prompt corrective action directive related to its safety and soundness or financial viability; or OTS informed the association that it is in troubled condition based on information available to OTS.)
- The savings association does not meet its regulatory capital requirements.
- The savings association commenced *de novo* operations within the past two years.



- OTS approved an application or notice under Part 574 involving the association or its holding company during the preceding two years.
- The savings association entered into a consent to merge or a supervisory agreement in the past two years.
- OTS or another banking agency has initiated a formal enforcement proceeding against the savings association and the proceeding is pending.

If OTS has imposed this notice requirement, the association must provide at least 30 days advance written notice to OTS before entering into any transaction with an affiliate or subsidiary. The notice must contain a full description of the proposed transaction. If OTS does not object during the 30-day period, the association may proceed with the transaction.

## TRANSACTIONS WITH INSIDERS

In addition to the affiliate transaction restrictions, you must verify an association's compliance with standards for extensions of credit to insiders. Section 563.43 applies FRB's Regulation O (12 CFR Part 215) to savings associations, their subsidiaries

Regulation O generally defines an extension of credit as making or renewing any loan, granting a line of credit, or extending credit in any manner.

and insiders (directors, executive officers, principal shareholders, and related interests). Specifically, § 563.43 applies the restrictions of 12 CFR Part 215, Subparts A and B (with the exception of § 215.13), to savings associations and their subsidiaries and insiders in the same

manner and to the same extent as if the association were a bank and a member bank of the Federal Reserve System.

## General Requirements

Regulation O applies various restrictions on extensions of credit to executive officers, directors, and principal shareholders of the association and its affiliates ("insiders") and to the related interests of these executive officers, directors, and principal shareholders. Beyond direct extensions of credit to insiders, an extension of credit is made to an insider if the proceeds of the extension of credit are transferred to the insider or used for the tangible economic benefit of the insider.<sup>3</sup>

Regulation O generally requires that most extensions of credit to insiders and their related interests meet the following criteria:

---

<sup>3</sup> There is an exception to the tangible economic benefit rule if both of the following criteria are met:

- The association extends the credit on terms prevailing at the time for comparable transactions with noninsiders (that would satisfy the standards set forth in § 215.4(a)) and that do not involve more than the normal risk of repayment).
- The borrower uses the proceeds of the extension of credit in a bona fide transaction to acquire property, goods, or services from the insider.

- Advance approval by a majority of the disinterested board of directors of the association.
- No preferential terms, does not involve more than the normal risk of repayment, and does not present other unfavorable features.
- Does not exceed aggregate individual and overall lending limits.

In addition, Regulation O imposes additional restrictions on extensions of credit to executive officers, and various reporting and recordkeeping requirements.

### Extension of Credit

Regulation O generally defines an extension of credit as making or renewing any loan, granting a line of credit, or extending credit in any manner. An extension of credit, as defined at § 215.3, includes the following transactions:

- A *purchase under repurchase agreement* of securities, other assets, or obligations.
- An *advance* by means of an overdraft, cash item, or otherwise.
- Issuance of a *standby letter of credit* (or other similar arrangement regardless of name or description) or an ineligible acceptance, as these terms are defined in § 208.24.
- An *acquisition by discount, purchase, exchange, or otherwise of any note, draft, bill of exchange*, or other evidence of indebtedness upon which an insider may be liable as maker, drawer, endorser, guarantor, or surety.
- An *increase of an existing indebtedness*, but not if the association advances additional funds for its own protection for any of the following:
  - Accrued interest.
  - Taxes, insurance, or other expenses incidental to the existing indebtedness.
- An *advance of unearned salary* or other unearned compensation for a period in excess of 30 days.
- Any *other similar transaction* that results in a person becoming obligated to pay money (or its equivalent) to an association, whether the obligation arises directly or indirectly, or because of an endorsement on an obligation or otherwise, or by any means whatsoever.

A transaction becomes an extension of credit at the time the association enters into a binding commitment to make the extension of credit. OTS considers a participation without recourse an extension of credit by the participating association, not by the originating bank or association.

---

Section 215.3 excludes certain transactions from the definition of an extension of credit. An extension of credit does not include any of the following transactions:

- An *advance against accrued salary or other accrued compensation*, or an advance for the payment of authorized travel or other expenses incurred or to be incurred on behalf of the association.
- A *receipt by an association of a check deposited in or delivered to the association in the usual course of business* unless it results in the carrying of a cash item for or the granting of an overdraft (other than an inadvertent overdraft in a limited amount that is promptly repaid, as described in § 215.4(e), which we discuss below).
- An *acquisition of a note, draft, bill of exchange, or other evidence of indebtedness* through any of the following means:
  - A merger or consolidation of depository institutions, or a similar transaction in which an association acquires assets and assumes liabilities of a bank, another association, or similar organization.
  - Foreclosure on collateral or similar proceeding for the protection of the association. The association, however, must not hold such indebtedness for more than three years from the date of the acquisition, unless OTS grants an extension for good cause.
- An *endorsement or guarantee for the protection of an association* of any loan or other asset the association previously acquired in good faith, or any indebtedness to an association for the purpose of protecting the association against loss or of giving financial assistance to it.
- *Indebtedness of \$15,000 or less* resulting from any general arrangement in which an association acquires charge or time credit accounts or makes payments to or on behalf of participants in a credit card plan, check credit plan, or similar open-ended credit plan, provided that both of the following conditions apply:
  - The indebtedness does not involve prior individual clearance or the association's approval other than to determine authority to participate in the arrangement and comply with any dollar limit under the arrangement.
  - The indebtedness is incurred under terms that are not more favorable than those offered to the general public.
- *Indebtedness of \$5,000 or less resulting from an existing or previously established interest-bearing overdraft credit plan* described in § 215.4(e), which we discuss below.
- A discount of promissory notes, bills of exchange, conditional sales contracts, or other similar paper, without recourse.

- Non-interest-bearing deposits to the credit of an association or bank are not considered loans, advances, or extensions of credit to the association or bank of deposit. The giving of immediate credit to an association or bank upon uncollected items received in the ordinary course of business is not considered a loan, advance, or extension of credit to the depositing association or bank.

## Insiders

Part 215 defines the terms executive officer, director, principal shareholder, and related interest, which we summarize below.

*It is important to note that Part 215 defines affiliate differently than §§ 23A and 23B as discussed earlier in this section under transactions with affiliates. Section 215.2(a) defines affiliate to include only the savings association's holding company, and any other subsidiary of that holding company. Similarly, § 215.2(c) defines "control" by a company or a person separately.*

### *Executive Officer (§ 215.2(e))*

Regulation O defines an executive officer of an association (or company) as a person who participates or has the authority to participate in the major policymaking functions of the association (or the company) regardless of title and regardless

Regulation O defines an executive officer as a person who participates or has the authority to participate in the major policymaking functions of the association (or company) regardless of title.

of whether the officer serves without salary or compensation. Insider does not include persons who may have official titles and exercise a measure of discretion in the performance of their duties, including discretion in the making of loans, but who do not participate in the major policymaking functions of the association or company. For example, the term executive officer does not include a manager or assistant manager of a branch of an association unless that individual participates, or the association authorizes that individual to participate, in major policymaking functions. Regulation O, however, presumes individuals with the following titles are executive officers of the association (or company):

- Chairman of the Board
- President
- Every Vice President
- Cashier
- Secretary
- Treasurer.

Regulation O does not generally consider directors, other than the Chairman of the Board, to be executive officers unless they serve in dual capacities as both a director and an executive officer.

Individuals presumed to be executive officers may be excluded from the definition of executive officer of the association (or company) if the following circumstances exist:

- A resolution of the board of directors or the bylaws of the association (or company), excludes the officer from participating in policy-making functions of the association (or company). The resolution or bylaws may list excluded individuals by name or title or may exclude a person by not including that person on a list of persons authorized to participate.
- The officer does not actually participate in policy-making functions of the association (or company).

Additionally, executive officers of an affiliate of an association are not subject to § 215.4 (General Prohibitions), § 215.6 (Prohibition on knowingly receiving extensions of credit), and § 215.8 (Records) if all of the following criteria are met:

- A resolution of the board of directors or the bylaws of the association, excludes the officer of the affiliate from participation in major policy-making functions of the association, and the executive officer does actually participate in such functions.
- The affiliate does not control the association.
- As determined annually, the assets of the affiliate do not constitute more than ten percent of the consolidated assets of the company that:
  - controls the association; and
  - is not controlled by any other company.
- The officer is not otherwise subject to §§ 215.4, 215.6, and 215.8.

#### *Director (§ 215.2(d))*

A director of an association or company includes any person who is designated as a director, or who performs duties as a director regardless of compensation. Director includes trustees, but does not include advisory directors, if they meet all of the following conditions:

- The shareholders do not elect them.
- They are not authorized to vote on matters before the board of directors.
- They provide solely general policy advice to the board of directors.

Directors of an affiliate of an association are not subject to § 215.4 (General prohibitions), § 215.6 (Prohibition on knowingly receiving extensions of credit), and § 215.8 (Records) if all of the following criteria are met:

- A resolution of the board of directors or the bylaws of the association excludes the director of the affiliate from participation in major policy-making functions of the association, and the director does not actually participate in such functions.
- The affiliate does not control the savings association.
- As determined annually, the assets of the affiliate do not constitute more than ten percent of the consolidated assets of the company that:
  - controls the association; and
  - is not controlled by any other company.
- The director is not otherwise subject to §§ 215.4, 215.6, and 215.8.

#### *Principal Shareholder (§ 215.2(m))*

A principal shareholder of an association does not include any company of which the association is a subsidiary.

Regulation O defines a principal shareholder of an association (or company) as a person (other than an insured association or insured bank) that directly or indirectly, or acting through or in concert with one or more persons, owns, controls, or has the power to vote more than ten percent of any class of voting securities of the association (or company). Shares that a member of an individual's immediate family (as defined at 215.2(g)) owns or controls are considered as held by the individual.

*A principal shareholder of an association does not include any company of which the association is a subsidiary. For example, principal shareholder excludes parent savings association holding companies.*

#### *Related Interests (§ 215.2(n))*

Regulation O defines a related interest of a person to include any company that the person controls. It also includes a political or campaign committee that the person controls, or the funds or services of a political or campaign committee that benefit that person.

### Restrictions on Extensions of Credit

Section 215.4 of Regulation O contains four restrictions on extensions of credit with insiders:

- Lending limits.
- Prior approval requirements.
- Qualitative factors.
- Overdraft provisions.

#### *Lending Limits (§§ 215.4(c) and 215.4(d))*

Regulation O imposes both an aggregate and an individual lending limit on extensions of credit to insiders.

#### Aggregate Lending Limit — General Limit

An association may not extend credit to any of its insiders or insiders of its affiliates in an amount that, when aggregated with the amount of all other extensions of credit by the association to all such insiders, exceeds the association's unimpaired capital and unimpaired surplus. In other words, the aggregate amount of all extensions of credit to all insiders may not exceed 100 percent of the association's unimpaired capital and surplus.

#### Aggregate Lending Limit — Small Savings Associations

Savings associations with less than \$100 million in deposits may make extensions of credit to insiders up to 200 percent of unimpaired capital and unimpaired surplus if all of the following circumstances exist:

- The board of directors determines by an annual resolution that a higher limit is consistent with safe and sound banking practices in light of the association's experience in lending to its insiders, and is necessary to attract or retain directors or to prevent restricting the availability of credit in small communities.
- The board resolution discloses the facts and reasons for the board's findings noted above, including the amount of insider extensions of credit as a percentage of unimpaired capital and unimpaired surplus as of the date of the board resolution.
- The association meets or exceeds all applicable capital requirements.
- The association received a satisfactory composite CAMELS rating in its most recent report of examination.

If the association subsequently fails to meet capital requirements or does not maintain a satisfactory composite rating, it cannot extend any additional credit (including a renewal of an existing extension of credit) to any insider of the association or its affiliates unless it is within the general aggregate lending limit.

### Exceptions to the Aggregate Lending Limit

The aggregate lending limits do not apply to extensions of credit that meet any of the criteria listed as follows. Extensions of credit that are:

- Secured by a perfected security interest in bonds, notes, certificates of indebtedness, or Treasury bills of the United States or in other such obligations fully guaranteed as to principal and interest by the United States.
- Extended to or secured by unconditional takeout commitments or guarantees of any department, agency, bureau, board, commission or establishment of the United States or any corporation wholly owned directly or indirectly by the United States.
- Secured by a perfected interest in a segregated deposit account in the lending savings association.
- Arise from the discount of negotiable or nonnegotiable installment consumer paper acquired from an insider that carries a full or partial recourse endorsement or guarantee by the insider, provided that it meets all of the following criteria:
  - The financial condition of each maker of such consumer paper is reasonably documented in the association's files or known to its officers.
  - An officer of the association designated for that purpose by the board of directors of the association certifies in writing that the association is relying primarily upon the responsibility of each maker for payment of the obligation and not upon any endorsement or guarantee by the insider.
  - The maker of the instrument is not an insider.

### Individual Lending Limit

An association may not extend credit to any of its insiders or to any insider of its affiliates in an amount that, when aggregated with the amount of all other extensions of credit by the association to that person and to all related interests of that person, exceeds the loans to one borrower (LTOB) lending limits.

The LTOB rule limits the total of all loans and extensions of credit by a savings association to one borrower, outstanding at one time, to 15 percent of the association's unimpaired capital and surplus. An association may extend an additional ten percent of unimpaired capital and surplus to one borrower if the additional amount comprises only loans and extensions of credit that are fully secured by readily marketable collateral. See 12 CFR § 560.93.

The National Banking Act (12 USC § 84(c) (1)-(10)) provides a list of ten exceptions to the percentage ceilings for certain secured extensions of credit. The additional exceptions to association LTOB



---

limitations contained in § 5(u) of HOLA are not available to compute the individual lending limit for extensions of credit to association insiders and related interests.

#### *Prior Board of Director Approval Requirement (§ 215.4(b))*

When the amount of an extension of credit exceeds certain thresholds, Regulation O requires prior board approval. In obtaining prior approval, all of the following actions must occur:

- A majority of the entire board of directors of the association approves the extension of credit in advance.
- The interested party abstains from participating directly or indirectly in the voting. Participation in the discussion or any attempt to influence the voting on the extension of credit will constitute indirect participation in the voting.

Prior approval, as described above, is not necessary for extensions of credit up to the higher of \$25,000 or five percent of the association's unimpaired capital and unimpaired surplus. However, prior approval is always necessary for extensions of credit over \$500,000. In determining compliance with these thresholds, the association must aggregate all extensions of credit to that person and to all related interests of that person.

Regulation O does not require board approval for any extension of credit the association makes pursuant to a line of credit the board of directors approved during the preceding 14 months.

Regulation O does not require board approval for an extension of credit the association makes pursuant to a line of credit the board of directors approved during the preceding 14 months.

#### *Qualitative Restrictions (§ 215.4(a))*

An association may not extend credit to any of its insiders or insiders of its affiliates unless the association makes the extension of credit on substantially the same terms (including interest rates and collateral) as those prevailing at the time for comparable transactions the association makes with other persons that are not insiders or otherwise employed by the association. The association must also follow its standard credit underwriting procedures, and cannot use less stringent underwriting procedures. Regulation O also requires that the extension of credit not involve more than the normal risk of repayment or present other unfavorable features.

This requirement does not prohibit an association from making a "preferential" extension of credit to an insider of the association (or its affiliate) if the association makes the extension of credit pursuant to an employee benefit or compensation program that is widely available to employees of the association (or the affiliate). The benefit program cannot give preference to any insider over other employees.

*Overdrafts (§ 215.4(e))*

An association may not pay an overdraft on an account of one of its executive officers or directors, or an executive officer or director of its affiliates. Exceptions include the payment of funds that are:

- Inadvertent, less than \$1,000 in the aggregate, overdrawn for five business days or less, and subject to the same fee charged to other customers in similar circumstances.
- Paid in accordance with a written, preauthorized, interest-bearing extension of credit plan that specifies a method of repayment.
- Funded by a written, preauthorized transfer of funds from another account of the account holder at the association.

**Additional Restrictions on Extensions of Credit to Executive Officers**

Additional restrictions apply to extensions of credit to the association's executive officers. Specifically, a savings association is prohibited from extending credit to its executive officers except in the amounts and for the purposes described below.

A saving association may extend credit to its own executive officers in any amount, subject to compliance with LTOB limitations, if the extension of credit is one of the following types:

- Finances the education of the executive officer's children.
- Finances or refinances the purchase, construction, maintenance, or improvement of a residence of the executive officer, provided two conditions occur:
  - A first lien on the residence secures the extension of credit and the executive officer owns the residence (or expects to own the residence after the extension of credit).
  - In the case of refinancing, the refinance amount includes only the amount used to repay the original extension of credit, together with the closing costs of the refinancing, and any additional amount used to finance the purchase, construction, maintenance, or improvement of a residence.

*Note:* Extensions of credit on vacation or second homes the executive officer owns or expects to own qualify as a residential loan, but only one loan to an executive officer may qualify for this category. Extensions of credit for other purposes, even if secured by a residence, either must fall within one of the other categories listed in these bullets or will be subject to limits on the "other purpose" loans under 12 CFR § 215.5(c)(4). The total outstanding amount of the other purpose category is subject to the dollar limits set forth below.

- Secured by a perfected security interest in bonds, notes, certificates of indebtedness, or Treasury bills of the United States, or in other such obligations fully guaranteed as to principal and interest by the United States.
- Secured by unconditional takeout commitments or guarantees of any department, agency, bureau, board, commission or establishment of the United States or any corporation wholly owned directly or indirectly by the United States.
- Secured by a perfected interest in a segregated deposit account in the lending savings association.

Section 215.5(c)(4) limits the aggregate loan amount for all other extensions of credit to the greater of 2.5 percent of unimpaired capital and unimpaired surplus or \$25,000, but in no event more than \$100,000. In addition, § 215.5(b) limits to these same amounts, extensions of credit to a partnership in which one or more of the association's executive officers are partners and, either individually or together, constitute a majority interest, regardless of the purpose of the extension of credit or the type of collateral. For purposes of this limitation, the total amount of the extension of credit to a partnership is attributed to each officer of the association, individually, who is also a member of the partnership.

A savings association must meet all of the following requirements when extending credit to an executive officer:

- Report the extension of credit promptly to the association's board of directors.
- Ensure that the extension of credit complies with the terms and creditworthiness standards of § 215.4(a) (that is, not on preferential terms or involve more than the normal risk of repayment or other unfavorable features).
- Obtain a detailed current financial statement from the borrower before extending credit.
- At the option of the association, make the extension of credit subject to a written condition that it become due and payable at any time the officer becomes indebted to any other bank(s) or association(s) in an aggregate amount greater than the permissible ceiling for a category of borrowings cited above (as outlined in § 215.5(c)).

### Miscellaneous Standards (§§ 215.6, 215.8, 215.9, 215.10, 215.11, and 215.12)

These sections and recordkeeping standards in Part 215 deal primarily with the reporting requirements for various transactions with insiders. Also, § 215.6 prohibits insiders from knowingly violating applicable restrictions on extensions of credit to insiders and related interests.

### Provisions Governing Indebtedness to Correspondent Banks

You should also determine whether an association complies with the provisions that generally prohibit preferential extensions of credit to insiders of correspondent banks and imposes certain recordkeeping requirements (See Appendix A).

### REFERENCES

#### United States Code (12 USC)

##### *National Banking Act*

§ 84(c) Lending Limits Exceptions

##### *Federal Reserve Act*

§ 371c Banking Affiliates (§ 23A of the FRA)

§ 371c-1 Restrictions on Transactions with Affiliates (§ 23B of the FRA)

§ 375a Loans to Executive Officers (§ 22(g) of the FRA)

§ 375b Extensions of Credit to Executive Officers, Directors and Principal Shareholders (§ 22(h) of the FRA)

##### *Home Owners' Loan Act*

§ 1467a Regulation of Holding Companies (§ 10 of the HOLA)

§ 1468 Transactions with Affiliates, Insider Loans (§ 11 of the HOLA)

##### *Bank Holding Company Act*

§ 1972(2)(H) Correspondent Accounts Definitions

#### United States Code (15 USCA)

##### *Investment Company Act*

80a-2(a)(20) Investment Adviser

## Code of Federal Regulations (12 CFR)

### OTS Regulations

- § 560.93                   Loans to One Borrower
- § 563.41                   Transactions with Affiliates
- § 563.43                   Loans by Savings Associations to Their Executive Officers, Directors and Principal Shareholders
- § 563.200                 Conflicts of Interest
- § 563.201                 Corporate Opportunity
- § 584.2-2                 Permissible Bank Holding Company Activities

### *Federal Reserve Board Regulations*

- Part 215                   Regulation O (Insider Loans)
- Part 223                   Regulation W (Transactions between Member Banks and Their Affiliates)
- §§ 225.24  
and 225.28                 Permissible Bank Holding Company Activities

**This page intentionally left blank**

# Transactions with Affiliates and Insiders Program

---

## EXAMINATION OBJECTIVES

Determine if transactions with affiliates (TWA) and insiders are in regulatory compliance and not detrimental to the safety and soundness of the savings association.

Evaluate the extent and degree of influence of affiliations on the savings association.

## EXAMINATION PROCEDURES

### LEVEL I

WKP. REF.

1. Review examination scoping materials related to transactions with affiliates and insiders. If another regulator performs the review of scoping materials, obtain a written or verbal summary of the review(s) concerning this program. Refer to the examiner-in-charge (EIC).

Scoping materials might include:

- The prior examination report.
- Prior exception sheets and work papers.
- Review of internal/external audit reports, supervisory analysis, correspondence, the business plan, minutes of the meetings of the board of directors, PERK information, etc.

- 
2. Review the preceding report of examination and all TWA-related exceptions and determine whether management has taken appropriate corrective action.

- 
3. Evaluate the savings association's policies and procedures for transactions with affiliates and insiders by reviewing policy statements, procedure manuals, board and committee minutes, and other pertinent documents.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

# Transactions with Affiliates and Insiders Program

---

WKP. REF.

4. Obtain and review the Management Questionnaire. Based on the review of minutes and any additional interviews with management, determine the completeness and accuracy of the answers to this questionnaire.
- 

5. Verify that transactions with affiliates and insiders are in compliance with applicable regulations:

- § 563.41 (applies the Board of Governors of the Federal Reserve System's (FRB) Regulation W at Part 223 to savings associations).
- § 563.43 (applies the FRB's Regulation O at Part 215 to savings associations).

*Note:* Appendix A, Regulation O Summary of Reporting/Recordkeeping Requirements, is a useful tool to determine regulatory compliance.

---

6. Evaluate the association's documentation and recordkeeping to determine compliance with minimum standards.
- 

7. Review Level II procedures and perform those necessary to test, support, and confirm conclusions derived from performance of Level I procedures.
- 

## LEVEL II

1. Evaluate the extent and degree of influence of outside affiliations on the savings association.
- 

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	



# Transactions with Affiliates and Insiders Program

---

WKP. REF.

2. From the review of information, determine which transactions, if any, you should review for evidence of self-dealing or conflicts of interest or other safety and soundness concerns. Provide instructions to the examiners reviewing the appropriate areas.
- 

3. Ensure that the examination meets the Objectives of this Handbook Section. State your findings, conclusions, and recommendations for any necessary corrective measures, on the appropriate work papers and report pages.
- 

## EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

<b>Exam Date:</b>	
<b>Prepared By:</b>	
<b>Reviewed By:</b>	
<b>Docket #:</b>	

**This page intentionally left blank**

---

REGULATION O SUMMARY OF REPORTING/  
RECORDKEEPING REQUIREMENTS

12 C.F.R. Section

Requirement

215.8

**Records of Institution**

A savings association must maintain records necessary for compliance with Regulation O. Any recordkeeping method adopted by the association must identify its insiders through an annual survey. The recordkeeping method must also identify insiders of affiliates through an annual survey; by a borrower inquiry method at the time the association makes an extension of credit; or by any alternative method acceptable to OTS.

The recordkeeping method adopted by the association must also include records of all extensions of credit to such persons, including the amount and terms of each extension of credit made to these persons and their related interests. Records must be sufficient to demonstrate compliance with applicable lending restrictions.

215.9

**Reports by Executive Officers**

Executive officers of the association must provide a written report to the association's board of directors within ten days of becoming indebted to any other bank or association in an aggregate amount that exceeds the amounts specified in § 215.5(c). The report must state the lender's name, the origination date, the amount of each extension of credit, the collateral or security for the debt, and the purpose of each extension of credit.

215.10

**Reports on Credit to Executive Officers**

An association must report in Schedule SI of its quarterly TFR all extensions of credit to its executive officers since the date of the previous TFR.

215.11

**Disclosure of Credit to Executive Officers and Principal Shareholders**

Upon written request from the public, the association must provide a list of outstanding extensions of credit to its executive officers, principal shareholders, and related interests of the executive officers and principal shareholders. The list must be as of the previous quarter end and should

include all aggregate extensions to one party and its related interests that are five percent or more of the association's capital and surplus or \$500,000, whichever is less. The association need not disclose specific amounts of individual extensions of credit. If the aggregate amount of all extensions of credit outstanding at such time to the executive officer or principal shareholder and the related interests does not exceed \$25,000, the association is not required to make a disclosure.

215.12 **Reporting Requirement for Credit Secured by Certain Bank Stock**

Executive officers or directors of associations whose shares are not publicly traded must annually report to the board of directors any outstanding credit that is secured by shares of the association.

215.22 **Reports by Executive Officers and Principal Shareholders or Their Related Interests**

On or before January 31 of each year, executive officers and principal shareholders must submit a written report to the board of directors regarding their outstanding extensions of credit from correspondent banks of the association. The association must notify executive officers and principal shareholders of this requirement, provide a list of the correspondent banks, and maintain the reports for three years. Associations may use FFIEC Form 004 (attachment to OTS TB 64-1c) or maintain the information in a similar format.

215.23 **Disclosure of Credit from Correspondent Banks to Executive Officers and Principal Shareholders**

Upon written request from the public, the association must provide the names of its executive officers, principal shareholders, and related interests that had outstanding extensions of credit from a correspondent bank at any time during the previous calendar year. The list must include the amount of the extension of credit if, when aggregated with all other outstanding extensions of credit from all correspondent banks to the executive officer or principal shareholder and the related interest, equaled or exceeded five percent of capital and surplus or \$500,000, whichever is less. The association need not disclose specific amounts of individual extensions of credit. If the aggregate amount of all extensions of credit outstanding from all correspondent banks to the executive officer or principal shareholder and its related interests does not exceed \$25,000 at any time during the calendar year; the association is not required to make a disclosure.