INTRODUCTION

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.

As the financial services industry continues to evolve, the duties of directors are becoming more complex and demanding. Today directors must take an active role in shaping and controlling a savings association's business operations and risks.

Responsibilities of the Board of Directors

The directorate has four basic responsibilities:

- To select qualified management and evaluate management’s performance.
- To establish business goals, standards, policies, and procedures.
- To review operating results and performance of new and existing activities.
- To ensure compliance with external standards, such as laws and regulations, and the association's own policies and procedures.

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

- Operate independently from management.
- Attend board meetings regularly.
- Avoid conflicts of interest and self-serving practices.
- Ensure that the association serves the credit needs of its community.

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 plan. In carrying out the evaluation, you should perform the following steps:

- 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 Handbook Section 320.

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.

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 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. In particular, reports should document any significant changes to capital, financial performance results, and major business activities. Management should provide such reports to directors before regular board or committee meetings to allow adequate time for review before the meetings.
- 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 with board-approved policies and directives.

The minutes should support the conclusions the directors reached in the meeting. Board 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.

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 appro-

priately. Undue reliance on only a few indicators may result in erroneous evaluations of the association's condition. 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.
- Selecting and employing a compliance officer who should be under the direction and control of the audit committee (not management).

All insured institutions with total assets of $500 million or more must have an independent audit yearly. See Section 350, Independent Audit. Ideally, independent auditors provide an objective look at the performance of the institution. 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 may also be part of a sound checks and balances system. It is the duty of this officer to monitor all association business transactions to ensure their compliance with regulatory provisions and their safety and soundness.

The internal 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. Capable management and personnel are the most important factors contributing to the success of the savings association.

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 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:

- Follows the board's direction and provides periodic reports to the board concerning policy compliance, such as interest rate risk exposure reports and earnings and capital projections and analysis.
- Periodically reviews the board's policies and, when appropriate, suggests changes.
- 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, non-accrual loans, real estate owned, and charge-offs and recoveries. Also reviews the adequacy of reserves and quantifies the effect of non-performing assets on the risk/return profile.
- Develops, reviews, and monitors capital plans, business 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 non-traditional banking activities or new business lines. 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

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.

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, capital raising efforts, major asset sales, boards of directors internal investigations, and defenses against regulatory determinations. The board of directors must justify and approve contracts that the association enters into with third parties.

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, and risk management. The Thrift Activities Handbook covers these areas in other Handbook 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 action. 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.

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 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. Option 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.

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 non-business 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.

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.

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 employ.
- 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, direc-

tors 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 pre-existing 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 circumcircumstances. OTS based 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 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.

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.
- Non-qualified “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

Savings associations with a composite CAMELS rating of 4 or 5 may enter into third-party contracts for services outside the normal course of business only with the regional director's pre-approval. Third-party contracts at failed associations frequently have been a waste of scarce resources. The regional director may establish a de minimis threshold amount to apply on a case-by-case basis. This requirement for regional director pre-approval 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 detrimental to the savings association or contrary to the public interest. They should receive close regulatory scrutiny since the costs may ultimately increase the cost of an association's failure to the 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 non-performance.
- 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 regional director will, within ten calendar days of receipt, notify an applicant association in writing whether it may 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.

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 rule would apply in the following situations:

- 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).
- Similarly, payments by the third party to a spouse, child, parent, sibling, or business partner of a person identified in the rule would generally provide a benefit to the person because of the personal or business relationship and would likewise be covered by the rule.
- In addition, a person who owes a fiduciary duty to an institution may not facilitate 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 a board member.

Sale of Covered Assets

As a result of FSLIC-assisted transactions, some associations have portfolios of covered assets. Covered assets are assets where the association receives yield maintenance payments and/or loss coverage upon disposition of the asset. The sale of covered assets to affiliated persons (defined in OTS regulation 12 CFR § 561.5) carries risk to the association and a potential cost to the FDIC. The sale of covered assets to such insiders raises the possibility of negative public perception of such transactions. Although the FDIC reviews the financial terms of all transactions involving covered assets, insider sales may appear as sweetheart deals, even if economically sound. Savings associations should not sell covered assets, as defined by FSLIC Assistance Agreements, to affiliated persons.

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. Examples of the types 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; and 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.
- Non-federally 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 request an FEC advisory opinion from the:

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 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 non-public information concerning their corporation. The misuse of material non-public 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 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 review carefully the riders thereto that might impair its

utility. The terms of these policies are negotiable. See Section 330, Management Assessment.

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

Office of Thrift Supervision 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 64-1d	Reporting of Loans from Correspondent Banks

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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.) 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?

5. 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?

6. Is there a concentration of board members and, therefore, a concentration of interests in certain businesses (such as real estate or construction)?

7. Determine whether there were any occurrences of self-dealing or conflicts of interest involving the board of directors.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

8. Complete the General Questionnaire, Oversight by the Board of Directors.

9. Determine whether the board of directors:

   - Delegates sufficient authority to management personnel to promote effective and efficient performance, and whether it retains sufficient control to discharge its responsibilities to stockholders, members, customers, OTS, and other regulatory authorities.
   - Is actively involved in directing the association's operations, and adequately monitors its performance.
   - Provides direction to management as to the development of an optimal risk/return profile.
   - 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.
   - Reviews the level and reasonableness of officers' salaries and affirms that they are commensurate with their experience and duties.
   - Provides adequate oversight of the personnel department and its policies.
   - Reports annually to the shareholders in the required format, if applicable.

10. 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

control, employee morale, or association performance. Ensure employee contracts meet the requirements of 12 CFR § 563.39.

11. 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.

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

Level II

13. 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?
- Are directors aware of significant regulatory changes enacted during the examination period?
- Has the board appointed a compliance officer?
- Did management consider the results of prior years' compliance reviews and examination reports when they designed procedures for the current compliance review?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Did the audit committee or the board review the results of the most recent compliance audit?
- 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?

14. 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?
- 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?

15. 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?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- 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?

16. 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?

17. Do the minutes reflect that the board, in reviewing higher-risk loans, explored efforts to minimize risk and limit the amount invested?

18. Has the board implemented an effective internal asset review function?

19. 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?

20. Do directors approve promotions and bonuses and document such approvals in the minutes?

21. 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

		Wkp. Ref.
	profitability?	
22.	Review directors' compensation for reasonableness. Consider peer group information and the time directors devote to the association's affairs.	
23.	Determine if operating committees are active between board meetings, and if the committees subsequently report their actions to the board for ratification.	
24.	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.	
25.	Review and consider the CAMELS rating in each area in determining your overall conclusions regarding the oversight by the board of directors.	
26.	Determine if there is a need to review any association transactions for evidence of self-dealing or conflicts of interest.	
27.	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.	

Examiner's Summary, Recommendations, and Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Oversight by the Board of Directors Questionnaire

General Questionnaire

Board of Directors - General Requirements

	Yes	No
1. Is the composition of the board within the guidelines of § 563.33(a)?		
2. Have all directors regularly attended directors' meetings during the year?.....		
3. 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?.....		
4. Has each director had the opportunity to review and modify all minutes of board and committee meetings during the period prior to approval?.....		
5. Are the minutes complete?.....		

Conflicts of Interest - 12 CFR § 563.200

	Yes	No
6. 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?.....		
• Do board members furnish written conflict-of-interest representations annually?		
• 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.).....		
• Has any director engaged in any transaction with the association or its affiliates that give the appearance of a conflict of interest?.....		

Reporting of Loans from Correspondent Banks - 12 CFR Part 215, § 563.43, TB 64-1c

	Yes	No
7. 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?		

Safety and Soundness Standards - 12 CFR Part 570

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

Annual Independent Audits and Reporting Requirements - 12 CFR Part 363

	Yes	No
10. 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?		
• Does the committee review with management and the independent public accountant the basis for the reports that 12 CFR Part 363 requires?		

Interest Rate Risk Management Procedures - 12 CFR § 563.176

	Yes	No
11. Does the board of directors (or a designated committee of the board) review the savings association's interest rate risk exposure? ..		
12. Has the board of directors formally adopted a policy for the management of interest rate risk?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Oversight by the Board of Directors
Questionnaire

	Yes	No
13. Does the board of directors periodically receive reports from management regarding implementation of the interest rate risk policy?		
14. 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?		
15. 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?		
Financial Derivatives - 12 CFR § 563.172		
16. Has the board of directors established written policies and procedures governing authorized financial derivatives?		
Supervisory Policy Statement on Investment Securities and End-User Derivatives Activity		
17. Has the board of directors approved major policies for conducting investment activities, including the establishment of risk limits? ...		
18. Does the board of review portfolio activity and risk levels, and require management to demonstrate compliance with approved risk limits?		
Interbank Liabilities - 12 CFR § 206.3		
19. Does the board of directors annually review and approve the association's interbank liability policies and procedures?		
Payment Systems Risk - 12 CFR § 210.25		
20. 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		
21. Does the board of directors, at least annually, review and approve lending policies for extensions of credit secured by real estate?		
22. Do the lending policies reflect risk levels that are acceptable to the board and provide clear and measurable underwriting standards?		
• 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?		
• 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?		
• 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?		
• Does the board review the status of all high-risk loans on a regular basis?		
Appraisal Policies and Practices of Savings Associations and Subordinate Organizations - 12 CFR § 564.8, TB 55a		
23. 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?		
24. Has the board of directors developed and formally approved written appraisal policies?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Oversight by the Board of Directors Questionnaire

	Yes	No
25. Does the board of director's annually review and approve appraisers for compliance with association policies, procedures and reasonableness of estimates?		
26. 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?		
Classification of Assets - 12 CFR § 560.160		
27. 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?		
Written Security Program - 12 CFR Part 528		
28. Has the board of directors developed and implemented a written security program for the association's main and branch offices?.		
Report of Condition - 12 USC § 1817(a)(3), TFR Instructions		
29. Do two or more members of the board of directors attest to the report?		
Report of Examination - ROE Instructions		
30. Do the directors review the report of examination and sign the Director's signature page for review during the next examination?		
Guidelines for Developing Adequate Control Practices and Responsibilities for End-User Computing Operations - TB 29		
31. Has the board of directors established appropriate policies that identify management responsibilities and control practices for all areas of information processing activities?		

	Yes	No
Client/Server Computer Systems - CEO Memo Number 59		
32. Has the board of directors developed and adopted appropriate policies, practices or procedures covering management's responsibilities and controls for all areas of client/server computing activities?		
Corporate Business Resumption and Information Systems Contingency Planning - CEO Memo Number 72		
33. Has the board of directors and senior management established policies and procedures to ensure that comprehensive corporate business resumption, contingency planning, and testing takes place?		
34. Does the board of directors annually review the adequacy of the association's business recovery and contingency plans and results of the tests, and document such review and approval in the board minutes?		
Executive Compensation and Employment Contract Oversight - 12 CFR § 563.39		
35. Does the board of directors annually review and approve all employment contracts and compensation arrangements for senior officers and directors?		
36. Has the board of directors defined the duties and responsibilities of the institution's managing officer in writing?		
37. 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?		
38. If the institution uses employment contracts, do they meet the requirements of § 563.39?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Oversight by the Board of Directors Questionnaire

	Yes	No
Bond Coverage for Directors, Officers, Employees, and Agents - 12 CFR § 563.190		
39. Does the board of directors formally approve and annually review and assess the association's standard and supplemental bond coverage?		
Retail On-Line Personal Computer Banking - CEO Memo Number 70		
40. If the association is contemplating (or engaging in) retail personal computer banking, has the board of directors and management established a comprehensive program to manage the inherent risks associated with such activities?		

	Yes	No
Retail Sales of Nondeposit Investment Products - TB 23-2		
41. 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?		
• 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?		
• 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?		

Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

INTRODUCTION

Meetings between regulatory staff and the board of directors – the individuals ultimately responsible for an institution's affairs – serve a variety of functions. They provide opportunity for interaction, and they facilitate long-term communication, which is especially important when the regulatory process reveals significant adverse information. Meetings help keep directors and regulators mutually informed by providing them an opportunity to discuss any of the following items:

- The examination process and findings.
- The institution, its functions, and plans.
- The general financial environment.
- Industry-related concerns.

Meetings give regulators an opportunity to obtain commitments from the board for corrective action.

Meetings with the board are distinct from management meetings, also known as exit conferences, closing conferences, or exit interviews. Examiners meet with executive management near the end of an examination to review overall findings and obtain commitments for corrective action. (See Thrift Activities Regulatory Handbook Section 070, Overall Conclusions.) The examiner in charge (EIC) should notify management of all examination-related items slated for discussion with the board, except recommendations to remove management.

TYPES OF MEETINGS

There are two primary types of meetings between regulators and the board: regular – those relating to examinations; and special – not primarily for presenting examination findings. However, a meeting can serve multiple purposes. For example, a regular meeting can serve to acquaint regulators with the board, enhance communication, and present findings.

Regular Meetings

A regular meeting can result from regular, special, or limited examinations. Its primary purpose is to discuss findings and agree on corrective action. A secondary purpose is to gather information regarding a new function for the institution. These meetings can also enhance the directors' understanding of the regulatory process and establish a rapport and build lines of communication with regulators.

You should consider attending a regularly scheduled board meeting that occurs during an examination. The purpose is not necessarily to discuss findings although it may be an opportunity to discuss scope and preliminary findings. The main objective, however; is to observe the board in action and establish a rapport.

If an institution's rating is adverse, you should arrange to meet with the board after the examination. Any of the following indicators denote an adverse rating:

- A composite rating of 4 or 5.
- A composite rating of 3 if the rating represents a downgrade from the previous examination.
- A CRA rating of Needs to Improve or Substantial Noncompliance.
- A Holding Company rating of Unsatisfactory.

Generally you should meet with the boards of all 3-rated institutions. However, the EIC, in concurrence with the field manager, determines whether it is necessary to meet if the 3 rating is not a downgrade from a prior examination.

Sometimes you might schedule a meeting with the board of an institution that does not have an adverse rating. This is appropriate when the EIC notes adverse trends, increased risk profile, or other matters that need to be brought to the board's attention. If no issues exist, the EIC

should honor any request from management to forgo a meeting.

If an institution's assets exceed $1 billion, you should schedule a meeting with the board regardless of adverse trends. The field manager must concur with any decision to forgo a meeting.

While you normally meet after the examination, you could arrange a regular meeting during the last week. This is appropriate if you have already discussed the examination results with management. Your meeting can also coincide with the board's next regularly scheduled meeting. You can mutually agree on another time to meet as long as that date is within 60 days of completing the examination. Also when scheduling, consider whether directors would benefit from receiving a copy of the report of examination (ROE) prior to the meeting.

The meeting agenda should include the following issues that warrant the board's attention:

- A comparison of the institution's policies, practices, and reporting systems with those of a well-managed, comparable institution.
- Corrective action taken by senior management.
- The institution's internal control system and internal audit coverage.
- The extent to which senior management and directors are receiving information needed to manage the institution effectively.
- Significant concerns regarding the quality of earnings.
- Management's long-term plans.
- Effectiveness of management personnel.
- The board's involvement in the institution's affairs.

Try to discuss ways to correct deficiencies without directing a course of action. If there are no major deficiencies, discuss the institution's overall condition and try to get the board's view of its future operations. Encourage directors to discuss matters that interest them.

Special Meetings

Reasons to schedule a special meeting include the following:

- To effect a supervisory action, such as a supervisory agreement or cease and desist order.
- To gather information in order to act on a proposal, application, or request by the institution.
- To discuss an institution's progress toward corrective action.
- To become acquainted following a change in directorate or a change in regulatory staff.
- To comply with directorate's request to meet.

MEETING PREPARATION, PRESENTATION, AND DOCUMENTATION

Prepare yourself thoroughly when meeting with the directorate. You should conduct yourself professionally and prepare sufficient documentation to ensure appropriate follow-up. A successful meeting will include all of the following steps:

- Preparation
  - — Ensure that the scheduling and selection of attendees satisfies the meeting's goal. See the discussion below on participation.
  - — Choose attendees and determine their responsibilities.
  - — Select a chairperson.
  - — Determine time and location.
  - — Develop an agenda. Refer to the discussion below.
  - — Notify participants of the meeting and its purpose.
  - — Meet with regulatory staff participants to discuss the agenda and other related issues.
  - — Prepare and organize supporting data, including comparative figures and ratios that

indicate trends and graphs to illustrate significant points or trends.

— Prepare any handouts or overheads for presentation.

- Presentation

— Conduct the meeting in a professional, objective fashion.

— Present the agenda (refer to discussion below) and follow it within reason.

— Establish good communication and maintain creditability.

— Encourage directors' involvement and solicit questions.

— Answer questions accurately. When unable to do so, refer inquiries to the OTS regional or Washington office.

— Obtain commitment from board to correct deficiencies, if appropriate.

- Documentation

— Evaluate and document results of the meeting. Refer to the discussion below.

Participation

You should meet with the entire board to ensure all directors are aware of regulatory findings and commitments to correct deficiencies. If all directors cannot attend, you can meet with a group, such as the audit, examination, or executive committee if:

- Outside directors are present.
- There are no material or adverse findings.
- The circumstances do not require a full board.

Honorary directors can participate in meeting discussions, but may not vote. Any person or organization connected with the institution, auditor, or holding company representative can attend the meeting upon board resolution. However, you can excuse such people if appropriate. As a rule, state supervisory authorities should attend meetings with the boards of state-chartered institutions.

EICs should meet regularly with the board. This allows them to discuss strengths and weaknesses noted during the examination and to answer any questions. Sometimes it is advantageous for the EIC to attend special meetings, too.

Agenda

To ensure an orderly meeting, you should prepare a detailed outline of discussion topics. The following outline is not all-inclusive but intended only as a guide:

Sample Agenda Outline

- Introductory remarks by regional office representative

— OTS policy regarding board meetings

— Purpose of meeting

— Type and scope of examination

- ROE results

— Overall condition of the institution

— Capital

— Asset quality, internal loan review, and reserves

— Management (including quality, depth, and continuity)

— Earnings

— Liquidity

— Funds management

— Sensitivity to market risk

— Internal controls and audit coverage

— Policies and procedures

— Reporting systems

— Management information systems

  - — Management reports to the board
  - — Reports of the board and committees
  - — Thrift Financial Reports
  - — Planning process
  - — Personnel
  - — Compliance systems
  - — Legislative and regulatory compliance (identify significant violations)
  - — Supervision by board
  - — Service corporation and holding company examination results
  - — Summary
- Corrective action (after discussion with appropriate regulatory staff)
  - — Summary of problems
  - — Board commitments
- Disclosure of ratings
- Other matters
- Questions from the board
- Overall conclusions

Documentation

After the meeting, prepare a memorandum to record results, date, time, location, and participant's names and titles. Describe the items discussed, the board's reactions, and any commitments for corrective action. If the board promises corrective action, send the memorandum to them for concurrence.

At the conclusion of any meeting conducted by the board (rather than the regulators), you should ask for a copy of the minutes and review them for accuracy.

Keep a copy of the post-meeting memorandum and agenda in the appropriate supervisory file. You should amend the institution's regulatory profile to reflect any changes or future commitments as a result of the meeting. See Thrift Activities Regulatory Handbook Section 050.

REFERENCE

Office of Thrift Supervision

OTS Thrift Safety and Soundness Report of Examination Instructions

INTRODUCTION

In this Section, management refers to executive officers, such as president, vice president, secretary, treasurer, or controller. It also refers to any persons, including division managers, who have the ability, with or without explicit authority, to implement and interpret the association's policies and procedures.

A major examination objective is to evaluate the quality and effectiveness of management. The success or failure of almost every facet of operations relates directly to management. Management develops procedures and strategies and makes decisions within the policies and guidelines that the board of directors establishes.

In evaluating management performance, you should consider the knowledge, skills, and abilities of the individuals, the results of their decisions, and the association's regulatory compliance and financial performance. There are a number of practices and procedures that management uses to control an association's activities that you must evaluate. These include, but are not limited to, planning, policy making, personnel administration, maintenance of internal controls, loan review, auditing, and maintenance of management information systems. You must consider the following management practices and procedures in your evaluation:

- A demonstrated willingness and technical ability to serve the legitimate banking needs of the community.
- Compliance with laws and regulations, including the adequacy of systems established to ensure compliance.
- Avoidance of conflicts of interest.
- Responsiveness to recommendations from auditors and supervisory authorities.

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.

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 of 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 relate to management deficiencies.

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

- There is soundness and consistency of objectives, policies, and procedures in the asset, liability, and operational areas.
- Personnel throughout the association adhere to policies.
- The association's management systems facilitate efficient operation and communications and monitor activities.

- The association's planning processes facilitate achievement of goals and objectives.
- 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.

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.

Prompt Corrective Action

Undercapitalized and significantly undercapitalized 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 who 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.

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
- 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. 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 27a provides compensation provision guidance and clarifies OTS policy about unsafe and unsound practices relating to executive compensation and employment contracts.

Planning

Sound planning is fundamental to effective management and is a key to anticipating and dealing with rapid change. Senior management and the board of directors should inventory the association's resources, examine changes in its operations, 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.

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 planning process.
- 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 and 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 or investment programs without appropriate planning, experience, 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 associations adherence to these conditions.

The Planning Process

To be effective, planning requires a structure and a process. Associations can segment planning into two classifications; 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.

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 training.
- 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. Use of a vendor or consultant does not lessen the burden on management to supervise and control the association's systems, policies and procedures. The savings association must have a written agreement with the vendor or consultant that outlines the conditions, rights, and responsibilities of each party.

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's 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.

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 bases 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.

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 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.

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 adversely affect an association's profitability 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.

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 affects 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 both 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 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 affiliate 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.

Internal Controls

Both the directors and senior management have important roles in an association's programs of internal control, loan review, and internal audit. 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. 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, 355, and 360 of this handbook.

Fidelity Bonds and Directors' and Officers' Liability Insurance

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 or EDP activities.
- The extent of coverage that a holding company fidelity bond or other affiliated entity provides.

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, em-

ployee, 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 security measures and controls is appropriate in every association. See the Compliance Activities Handbook Section 405, 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.

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.

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

Office of Thrift Supervision Bulletins

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

FFIEC Interagency Policy Statement

Interagency Policy Statement on the Internal Audit Function and Its Outsourcing

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 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.

2. Review the following records:

   - Organization chart. Identify key decision-making personnel (include copy in the continuing examination file).

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- 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 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.

4. 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.

   - Internal audit and loan review reports.

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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

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

Level II

8. Complete General Questionnaire 330, Management Assessment.

9. 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.

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

11. 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.

12. 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?

13. 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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- An assessment of the association's employee screening policies to determine that they are appropriate to protect the safety and soundness of the association.

14. 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?

15. 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.

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

17. Ask the managing officer or personnel officer if any employees or former employees have brought any discrimination complaints, lawsuits, workers compensation claims, unemployment claims, or wrongful discharge suits against the association during the review period. Compare the responses with the answer in the Management Questionnaire.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

18. 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.
- 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.

19. 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

20. 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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.

21. 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.

22. 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.

Examiner's Summary, Recommendations, and Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Management Assessment Questionnaire

General Questionnaire	Yes	No
1. Has the board set overall objectives for management performance and has management met the objectives?		
2. Does the institution have an organizational chart? If not, have lines of authority and reporting responsibility been formally established?		
3. Does senior management receive:		
• A brief statement of condition daily?		
• A daily liquidity report?		
• A list of assets subject to internal classification at least monthly?		
• A comparative earnings statement, at least monthly?		
4. Does management periodically review the institution'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?		
• Adequately deters irregularities by ensuring their timely detection?		
• Establish and maintain appropriate accountability?		
• Ensure the maintenance of well-planned records?		
• Ensure the segregation of duties?		

	Yes	No
5. Does the auditing function cover officers' compliance with board and management policies?		
6. Does the association have policies to ensure the continuity of development and depth of management personnel?		
7. Is the staff adequate to facilitate efficient operations?		
8. Does the institution comply with applicable statutes, regulations, and policy statements?		
9. Does the institution use a system of written job descriptions and performance standards, including descriptions for supervisory personnel?		
10. Does the institution perform background investigations on new employees?		
11. Does the association have a formal training program?		
12. Does the association provide management training to those persons likely to assume higher level positions?		
13. When appropriate, do employment termination procedures prevent a terminated employee's ability to control assets and records, eliminate passwords, change locks, remove signature authorities, and provide proper termination notifications to affected employees?		
14. If the institution was or is subject to the notification requirement 12 CFR § 563.550 is the institution in compliance with the regulation?		
15. If the institution 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?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Management Assessment Questionnaire

	Yes	No
16. Do the institution's executive compensation and employment contracts comply with 12 CFR § 563.39, § 563.161, and OTS policy set forth in Regulatory Bulletin 27a?.....		
17. Is the quality, quantity, and timeliness of the institution's management information systems adequate?.....		
18. Is management responsive, in a timely manner, to supervisory criticism?.....		
19. Is the institution in compliance with the restrictions of OTS regulation § 563.43, concerning loans to officers, directors, and principal shareholders?.....		
20. Are management's assumptions, analyses, and conclusions regarding the appropriate fidelity bond form and level of coverage reasonable and acceptable?.....		

Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

INTRODUCTION

OTS requires all institutions, 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.

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.

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 institution's reputation.
- Adherence to internal policies and procedures.
- Efficient operations.

A system of strong internal control is the backbone of an institution's management program. Strong internal control helps an institution 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 institution. 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 institution failures. Some institutions 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 control 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 regulatory) on internal control over financial reporting and compliance with certain laws and regulations, as well as filing annual audited statements under section 112 or FDICIA.

The board is also responsible for approving and periodically reviewing the overall business strategy and significant policies of the institution, as well as understanding the major risks the institution 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 institutions 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 institution, 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 Section 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 institution's control consciousness. The following parameters determine effectiveness:

- The extent of its involvement in and its scrutiny of the institution'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 institution 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 institution'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 institution'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 institution, 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 institution'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 institution'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 GAAS. 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 institution 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.

Note, however, that the five components do not reflect how the institution considers and implements internal control.

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 components listed above.

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:

- Conduct management inquiries.
- Inspect documents and reports to review how staff performs controls.
- Observe directly how management applies the controls.
- Retest how management applies the controls.

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.
- 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 institution'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 institution 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 institution will rectify its internal control deficiencies.

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 institution'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 stan-

dards 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 institution must have an organizational structure that supports its objectives. Management must plan, execute, control, and monitor institution 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 institution'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 institution'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 memo-

randa 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 institution, 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.

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 institution 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 institution, fraud detection is certainly a goal when reviewing an institution's internal control system. Recent problems concerning insiders at some institutions 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 institution 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. Should you encounter any red flags you should bring the situation to the attention of Regional Accountant. For more information, see Thrift Activities 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 institution is to assess the extent to which management has established internal control procedures and programs to identify and mitigate the institution'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 institution's external audit firm lacks savings association or bank audit experience, or the auditors assigned have limited experience.
- The institution enters new areas of activity without first implementing proper controls, or engages in new activities without experienced staff and appropriate controls in place.
- The institution fails to provide adequate reports to the board of directors.
- The institution does not have proper controls in high-risk areas.
- The institution often deviates from board-approved policies with exception documentation.
- The institution 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 institution has an effective internal audit function. Incorporate the following five basic components of SAS No. 78, discussed in detail in the next section, to assist your review of the effectiveness of the institution's internal control system:

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

Management's Responses

OTS sends questionnaires to the institution as part of the PERK. Institution 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 institution'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 institution'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 institution'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 institution 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 institution outsources any significant activities and Level I procedures are insufficient to determine how the institution 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

Institutions 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 institution to additional risks.

Outsourcing involves some of the same operational risks that arise when an institution

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 institution that bears the risk of financial loss, damage to its reputation, or other adverse consequences.

OTS expects institutions to ensure that controls over outsourced activities are equivalent to those that the institution would implement if they conducted the activity internally. The institution'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)

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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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.

12. 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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

13. 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.

14. 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.

15. Assess the adequacy of information and communication systems.

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

17. 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.)

18. 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.

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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

21. 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.

22. Verify cash on hand. Review cash items or any other assets or liabilities held in suspense accounts to determine proper and timely disposition.

23. 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.

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

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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

27. Check supporting documentation for loans charged-off.

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

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

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

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

32. 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.

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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

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

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

Examiner's Summary, Recommendations, and Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

QUESTIONNAIRES

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 Thrift Activities Regulatory 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 materialmens' lien wavers, 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 Thrift Activities Regulatory 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 a 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 Section 10 of the Federal Financial Institutions Examination Counsel (FFIEC) Information Systems (IS) Examination Handbook used by OTS. 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 Thrift Activities Regulatory 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 reconcilement 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.

THIS BLANK INTENTIONALLY LEFT BLANK

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

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

_____	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

_____	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
_____	24. Are procedures adequate to ensure that the association monitors and clears uncollected items?	_____	_____
	Person responsible? _____		
_____	25. If the association maintains a petty cash fund, are all additions and withdrawals documented?	_____	_____
_____	26. Does the association balance the petty cash fund periodically?	_____	_____
_____	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?	_____	_____
_____	28. Does the association record cash items appropriately in the general ledger?	_____	_____
_____	29. Does the association review teller and accounting system override reports and file maintenance summaries for unusual activity on a regular basis?	_____	_____
	Person responsible for accounting overrides? _____		
	Person responsible for teller overrides? _____		
_____	30. Are loan accounting systems included in the override reports?	_____	_____
_____	31. Are personnel who have control over cash barred from performing overrides?	_____	_____
_____	32. Do only designated personnel who have no control over cash approve and review overrides?	_____	_____
_____	33. Does the association, at both home and branch offices, perform daily cash reconciliations?	_____	_____
_____	34. Does a person without teller responsibilities perform the daily cash counts?	_____	_____
_____	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

_____	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
_____	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?	_____	_____
	If so, what is the amount? _____		
_____	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?	_____	_____
_____	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?	_____	_____
	Person responsible? _____		
_____	46. Is the supply of unused checks periodically reconciled to the shipping invoice by persons without signature authority?	_____	_____
	Person responsible? _____		
	How often? _____		
_____	47. Does a person independent of the check writing function review the paid (canceled) checks for proper signatures and reconcile the check to vouchers?	_____	_____
	Person responsible? _____		
	How often? _____		
_____	48. Does the association periodically reconcile outstanding checks to vouchers and liability accounts?	_____	_____
_____	49. Does the association periodically transfer all outstanding six-month old association checks to a liability account?	_____	_____

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

_____	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

Investments and Securities

_____	58.	Is documentation supporting account entries, broker's advice, and journal entries received and maintained by a person independent of the authorized trading officer?	_____	_____
_____	59.	Does the association maintain an investment security ledger or worksheet that details all securities held and all security transactions?	_____	_____
_____	60.	Are the security ledger totals for principal and accrued interest, balanced to the general ledger at least monthly by an independent person?	_____	_____
		➧ Person responsible? _____		
_____	61.	Does the association have procedures to ensure that they collect all income due on the investment security portfolio promptly?	_____	_____
_____	62.	Does the association have procedures that will indicate any relationship between brokers who purchase securities for the association and association officers, directors, or employees?	_____	_____
_____	63.	If the board of directors authorized an officer to have sole authority to purchase and sell securities, is the authority limited to fixed dollar amounts, above which a second officer must approve the transaction before its commitment?	_____	_____
		➧ Authorized person(s): _____		
		➧ Limits: _____		
_____	64.	Does the association prohibit broker/dealers from having discretionary trading authority?	_____	_____
_____	65.	Does the association place all orders only with broker/dealers not affiliated with investment advisors retained by the association?	_____	_____
_____	66.	Does the association engage in reverse repurchase agreements and lending of securities only with firms designated by the Federal Reserve Board as primary dealers in government securities?	_____	_____

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

_____	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

_____	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

_____	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

_____	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

_____	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

_____	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

_____	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.)

_____	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? 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

_____	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

_____	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

_____	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

_____	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

_____	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

_____	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

_____	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

_____	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.)

_____	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

_____	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

Funds Transfer and Wire Transfer 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? _____ _____

_____ 6. Do personnel consistently follow the procedures? _____ _____

_____ 7. Who is responsible for supervising the wire transfer activity to ensure compliance with the written procedures? _____

_____ 8. Is an internal or independent audit performed of the wire transfer procedures? _____ _____

_____ 9. Does the association provide adequate training to personnel involved with the wire transfer process? _____ _____

FUNDS TRANSFER QUESTIONNAIRE
Preliminary Examination Response Kit
Office of Thrift Supervision

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

Verified By Examiner		Yes	No
_____	10. Does the association segregate securities-transaction-related duties among the buyer/seller, the trader, and settlement clerk?	_____	_____
_____	11. Are dual authorizations (maker, approver) required before the sending department acts upon internal wire transfer requests?	_____	_____
_____	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?	_____	_____
_____	13. Do personnel involved with wire transfers receive proper background screenings, including criminal record investigation?	_____	_____
_____	14. Are sendable funds limited by using separate correspondent accounts to send and to receive funds?	_____	_____
_____	15. Are controls to limit daylight overdrafts effective?	_____	_____
	Briefly describe the controls: _____		
_____	16. Does the association audit the wire transfer log periodically?	_____	_____
_____	17. Does the association keep a complete log of wire transfer activity for audit?	_____	_____
_____	18. Does software provide a log of all wire transfer activity?	_____	_____
_____	19. If a data terminal is used, is an unbroken paper printout copy of all activity reconciled to requests daily?	_____	_____
_____	20. Are interim daily reconcilements and end-of-day reconcilements performed with all reconciling items cleared?	_____	_____
_____	21. Does the association prohibit the person who performs end-of-day balancing from executing wire transfers?	_____	_____
_____	22. Is the person who executes wire transfers prohibited from access to cash (such as having a teller drawer)?	_____	_____

FUNDS TRANSFER QUESTIONNAIRE
Preliminary Examination Response Kit
Office of Thrift Supervision

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

Verified By Examiner		Yes	No
_____	23. Does the association prohibit the person who reconciles the association's deposit account affected by wire transfer activity from executing wire transfers?	_____	_____
_____	24. 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?	_____	_____
_____	25. 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?	_____	_____
_____	26. Does the association restrict access to test codes to only those employees authorized to handle wire transfer requests?	_____	_____
	27. Does the association keep the test codes in a secure place?	_____	_____
_____	28. If the association uses code words do they change them periodically?	_____	_____
	How often? _____		
_____	29. Does the association strictly forbid the transfer of uncollected funds?	_____	_____
_____	30. Does the association require dual officer approval for large-dollar transfers?	_____	_____
	Who is authorized and what are the limits? _____		
_____	31. Does the association require customer and/or bank verification callbacks for voice wire transfers above an established dollar threshold?	_____	_____
	Who is responsible for verification? _____		
_____	32. Does the association make all securities-transaction-related transfers only after the verified receipt of securities (delivery versus payment)?	_____	_____
_____	33. Does a person independent of the transaction approval or processing balance wire transfers at least daily?	_____	_____

FUNDS TRANSFER QUESTIONNAIRE
Preliminary Examination Response Kit
Office of Thrift Supervision

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

Verified By Examiner		Yes	No
_____	34. 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 sire instructions?	_____	_____
_____	35. 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)?	_____	_____
_____	36. Does the association require that customer wire-transfer requests be in writing and signed by the customer wiring the funds?	_____	_____

Wire Transfers Using Personal Computer Systems

_____	37. Does the association keep the personal computer executing wire transfers in an area that is physically secure from unauthorized employees and the public?	_____	_____
_____	38. Does each authorized user of the wire transfer system have a unique password known only to that user?	_____	_____
_____	39. Do separate persons enter and release outgoing transfers with separate unique passwords?	_____	_____
_____	40. Do employees adequately protect passwords to ensure that only the authorized user is aware of the password?	_____	_____
_____	41. Does the system require users to change their password periodically?	_____	_____

FUNDS TRANSFER QUESTIONNAIRE
Preliminary Examination Response Kit
Office of Thrift Supervision

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

Verified By Examiner		Yes	No
_____	42. 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? ___		
_____	43. 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?	_____	_____

Branch Procedures (Customer-Requested Wire Transfers)

_____	44. Does a branch procedures manual contain a clear and concise description of branch wire transfer procedures?	_____	_____
_____	45. Are telephone requests from the branch office to the main office for two-party wire transfers accepted?	_____	_____
_____	46. Briefly, describe the procedures the association uses to ensure that such requests are authentic. _____		
_____	47. Does the association identify all transfers by sequential code or encrypted passwords in prearranged order with correspondents?	_____	_____
_____	48. Are third-party wire transfers by telephone confirmed by four-person call-back procedure (sender, receiver, approver, confirmer)?	_____	_____
_____	49. Does the association record all calls?	_____	_____
_____	50. Does each participant document callbacks?	_____	_____
_____	51. Is a signed customer-authorization form required as a source document and proof of authorization for customer-requested wire transfers?	_____	_____
_____	52. 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?	_____	_____
_____	53. Does the association retain customer authorization forms?	_____	_____

FUNDS TRANSFER QUESTIONNAIRE
Preliminary Examination Response Kit
Office of Thrift Supervision

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

Verified By Examiner		Yes	No

Internally Generated Wire Transfers (Department Requests for Wire Transfers)

_____	54.	Does the association require that all departmental wire transfer requests be in writing, on a preprinted form?	_____	_____
_____	55.	Does the request form contain all necessary from-account and to-account information?	_____	_____
_____	56.	Do departmental request forms indicate the initials or signatures of the initiator and approver who authorized the wire transfer?	_____	_____
_____	57.	Do separate persons originate, approve, and send internally generated wire transfers?	_____	_____
_____	58.	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?	_____	_____
_____	59.	Recommend any improvements needed to prevent individuals from transferring funds to another's account while acting alone.	_____	_____

Prepared By: _____

Verified By: _____

INTRODUCTION

Financial institutions operate in a technology-intensive industry. Almost all aspects of operations are automated and most business transactions are consummated without the exchange of currency. Instead, transactions are stored, processed, and transported electronically using information systems and technology.

Financial institutions have long stored information in electronic form. Historically, however, transaction entry remained largely a manual process, providing a traditional paper trail through which the accuracy of electronically produced output reports could be verified. Today, advancements in communication technology are increasingly replacing institution-controlled, paper-documented transactions with electronic entries initiated by customers, by telephone or PC, by merchants, through automated bill payment, etc. Financial institutions need new methods to control transaction input, to ensure its accuracy.

Institutions are also becoming more dependent on electronic information to make strategic and daily management decisions. Institutions use computer models to:

- Develop budget projections and business plans.
- To underwrite loans.
- To measure interest rate risk.
- To manage assets.
- To track trust accounts.
- To produce loan documents and consumer protection disclosures.
- To measure management performance.
- Manage virtually every other aspect of financial institution activities.

Increasingly, institutions download electronic data from third parties, such as credit bureaus, and run that data through a variety of internal electronic decision models. Institutions use the results to determine:

- Where to market their products.
- How to price them.
- Who to grant loans to.
- What the terms should be.
- When to cross-market other products.
- When to adjust credit limits or interest rates on individual accounts and by how much.
- To determine the most effective collection strategy.

As this dependence on electronic information grows, it is increasingly important to take appropriate measures to ensure the integrity of the input, to protect against corruption of the data or the programming, and to test the accuracy of the output.

Risks are inherent in all electronic capabilities. Threats can come from both internal and external sources. Outside hackers, disgruntled employees, and inadvertent errors can adversely affect reliability. Unauthorized parties may inappropriately alter Web sites or hackers may initiate denial of service attacks to prevent customers from transacting business. Electronic mail containing confidential or proprietary information may be distributed in error. Unauthorized parties might access networked systems that are directly connected to an institution's main operations database, revealing sensitive data.

At the same time, traditional information integrity and availability responsibilities and risks continue to be present. Management's responsibility to protect records from fires and natural disasters predates what we call technology, but the responsibility to safeguard the confidentiality of customers' records is the same whether that means physically restricting access to ledger cards and file vaults or establishing and maintaining logical access controls such as strong password and log-on practices to protect information stored in electronic form.

Institutions increasingly are seeking control enhancements to mitigate risks that impact data integrity and data availability, and provide new opportunities to remain competitive, enhance profitability, and improve customer service. Recent lessons learned from Year 2000 renovation work, use of the Internet as an alternate delivery channel, and regulators' emphasis on risk management processes are prompting institutions to give greater attention to planning for use and control of information technology.

The Year 2000 project was one of the most expensive and resource-intensive information technology challenges ever faced by the financial services industry. The project posed a technology-based problem that had to be managed on an enterprise-wide basis by more than technology experts. It transcended corporate boundaries and hierarchies and required organizations to work together to review information technology (IT) systems and business practices and develop a comprehensive strategy to address technology related risks and business continuity plans.

The financial institutions best prepared for Year 2000 shared common characteristics. Typically, these institutions:

- Had senior managers and directors who were committed to and involved in the project.
- Used interdisciplinary teams.
- Developed comprehensive IT inventories.
- Improved their vendor management practices.
- Prepared and tested detailed contingency plans.
- Strengthened internal controls and security.

These practices are also essential to the ongoing prudent management of information technology.

This handbook section, which supplements Section 340, Internal Control, describes a safety and soundness examination program to evaluate technology risk controls. If management does not identify and address technology risks, problems such as unauthorized access to records, data integrity deficiencies, inadequate disaster contingency planning, interruption of customer service, lack of internal controls, and fraud can cause significant losses for the institution. You can use this examination program to determine if an institution's controls are adequate to reasonably ensure a safe, sound, and secure infrastructure for use of information technology. We generally refer to "you" as the safety and soundness examiner. When necessary, we make the distinction between Safety and Soundness (S&S) and Information Technology (IT) examiners.

INFORMATION TECHNOLOGY IN THRIFT INSTITUTIONS

Financial institutions have a number of choices available to meet their information systems and technology needs. Most OTS-regulated thrifts outsource most of their data processing functions to one or more third-party service providers; these are sometimes called "serviced thrifts." A much smaller portion of thrifts maintain internal data centers to run software licensed from vendors or developed in-house. Mixes or hybrids of these basic approaches are common. A thrift might contract with one service provider for its general ledger and deposit systems, with a second service provider for loans, and with a third for its web site. The same thrift might use licensed software for certain investments and interest rate risk analysis and might use complex spreadsheets developed in-house for some asset quality and board reports.

In addition to doing business with the primary and secondary service providers, most thrifts are interconnected with various other entities, such as ATM networks and automated clearing houses (ACHs), to process daily business. And, most thrifts now maintain one or more internal networks known as Local Area Networks (LANs) or Wide Area Networks (WANs). More and more of the internal networks are configured in a client-server environment.

Each of these arrangements requires a different type and level of management involvement with regard to data integrity controls, security measures, and business continuity plans.

Outsourcing

Almost all thrift institutions, including large entities, use outsourcing to some extent.

Contracts with service providers typically provide for a standard package of routine and standardized services and reports and allow for some special reports. Additional costs may be incurred for certain special reports or for nonstandard processing of standard reports.

Client institutions may request services and products beyond those provided for in the contract, for example, for a new deposit or loan product. Clients generally must pay extra for unique software requirements that are not enhancement priorities to the provider/ vendor and client-base at large. In these situations, institutions frequently build their own supplemental systems (for example, using PC-based applications) to augment outside products and services.

The delegation of data processing or other technological functions to a third party requires reasonable due diligence in selecting and contracting with service providers and vendors, and in monitoring performance. Conditions, rights, and responsibilities of the institution and the third-party service provider or vendor should be governed by written agreements. This is particularly important in an electronic environment because short-term engagements, new developments, and untested entities are not uncommon. Further, management must coordinate all outsourcing arrangements to ensure that security, reliability, and integrity are not compromised.

Independent Service Providers

Contracting with independent service providers is common at thrifts of all sizes. An independent service provider can provide experienced staff, proven software, and reliable hardware that might otherwise be difficult if not cost-prohibitive for an individual thrift to maintain. However, the selection of an independent service provider is important. Most contracts are long-term, and it is important that the institution ensure that the service provider can deliver the appropriate type and quality of service that the institution will need over the life of the contract. If the service provider does not provide the needed services, or cannot promptly add services the institution needs later to meet market conditions, it may constrain the institution's operations. For example, its choice of loan products may be more limited than what changing competitive factors might otherwise dictate.

Similarly, dissatisfaction with a service provider will typically lead to a conversion from one data service provider to another. While converting to a service provider that better meets the institution's needs is a business decision, and not automatically a regulatory concern, conversions can be disruptive to the normal flow of business. Fees or penalties for early contract termination can be considerable. Appropriate upfront due diligence and planning should help institutions avoid unnecessary conversions.

Most serviced thrifts have one primary service provider and one or more secondary service providers. Typically, the primary service provider is responsible for (and paid for) ensuring compatible setups, connections and data transmissions with the secondary service providers as well as with other companies and entities included under the technology umbrella (for example, the ATM network).

Data is forwarded to the service provider's computer center, usually via on-line data entry terminals. Output reports are available at the institution's on-line terminals and printers, or in some cases, or for certain reports, hardcopy or microfiche reports may be delivered.

Client institutions are responsible for establishing and maintaining appropriate controls over those portions of the serviced systems that are under their control. For example, institutions should permit only tellers and other authorized personnel to use teller terminals. Other common controls that clients, rather than service providers, are responsible for include certain balancing and reconciling activities. Client responsibilities should be addressed in the contract and may be discussed in greater detail in other documentation from the service providers or independent auditors conducting third-party reviews (discussed later). Thrift management is also responsible for ensuring that employees are properly trained on the systems they use and related control steps.

Affiliated Service Providers

Thrifts that are part of a holding company structure may have an affiliated company handle their technological needs. This may be a department of the holding company or a separate affiliated company. This frequently happens where there are several financial institutions with common ownership. The related institutions can eliminate some duplication of efforts and equipment and realize economies of scale.

Where there are such contracts or arrangements, Transactions with Affiliates provisions may apply. For additional information, see Section 380 of this Handbook.

In-House Computer Centers

In-house computer centers vary in size and complexity. Computer equipment may vary in size from large "mainframe" to smaller microcomputer systems. Also, the level of responsibility assumed by the institution can vary. Under the traditional in-house computer arrangement, the thrift would own the hardware and would be responsible for developing, maintaining, and operating the program. However, most banks and thrifts have implemented a hybrid arrangement, where they outsource some of the responsibilities traditionally associated with in-house systems.

One type of hybrid arrangement is often referred to as a turnkey operation. Under this type of set up, thrifts will acquire software from a third party, and run the software on equipment owned and operated by the thrift. One variation of a turnkey operation is when a thrift enhances the standard software to better suit their information needs. The additional programming is referred to as "surround code."

Facilities management is another type of IT environment occasionally seen in financial institutions. In these cases, the financial institution has an in-house data center, but employees of a service provider provide the programming and operate the systems.

Other "Internal" Technologies

Whether the institution's main data processing functions are handled internally or outsourced, some technologies common to most financial institutions have emerged in recent years.

End-User Computing

With the advent of PCs, thrift officers and employees began creating applications to supplement those provided by service providers or internal data centers. As PCs and software applications simultaneously became more powerful and easy to use, and downloading information from service providers and in-house data centers became more feasible, these business users, as opposed to IT professionals, created yet more complex "end-user" applications.

These business users may create new software programs or miniprograms or customize existing routines from vendor software. PC users originate data, download and manipulate information from main databases, and upload data to secure databases. Each of these activities can create information that management may use to make decisions that affect corporate strategies, customer relationships, and governmental reporting.

Management should take steps to implement and maintain control techniques for the programming, testing and documentation of end-user applications to ensure the integrity of the software and the production of accurate reports. TB 29, End-User Computing, contains more detailed guidance on basic controls that should be implemented and maintained in this area.

Computer Networks

The power of PCs also helped information processing to evolve well beyond the traditional central environment to decentralized or distributed networked operations. Most OTS-regulated thrifts have at least one internal network of PCs, whether the thrift is serviced or operates an in-house data center.

Computer networks offer substantial benefits in productivity and information access. A Local Area Network or LAN refers to a network that

interconnects systems within a small geographic area such as a building, or even just a floor or portion of a building. Through PCs or other terminals, users have access to common systems, databases and software; communicate via electronic mail (email), and share peripherals such as printers. A Wide Area Network or WAN is a wider network that connects users in other locations. A thrift might have a LAN within its headquarters building and a WAN for its branches to communicate with each other and the home office. Other types of computer networks include MANs (Metropolitan Area Networks) and VPNs (Virtual Private Networks).

These networks provide high-speed interconnection and data exchange and facilitate communications within the institution and between the institution and the users (staff and customers). Some familiar online customer delivery application systems that are available to network users include telephone banking, PC banking, ATMs, automatic bill payments, and automated clearinghouse (ACH) systems for direct deposit or payment.

Institutions using LANs, WANs, or other types of computer networks need to have policies and procedures that govern the purchase and maintenance of hardware and software. They must also establish and maintain sound controls that allow reasonable access to data but also protect data's confidentiality and integrity.

For more detailed guidance, see CEO Memorandum No. 59, Risk Management of Client/Server Systems, which forwarded the interagency statement on this topic.

Electronic Banking and Internet Activities

Electronic banking encompasses customer services such as telephone banking and PC banking, whether the latter is conducted through a direct connection or over the Internet. General Internet activity refers to activity by thrift employees including browsing, downloading, or other Internet activity, using institution resources for purposes not related to the institution's Internet banking products.

Institutions that have any sort of electronic banking or Internet activities should be prepared to deal with unique information security matters through the advice and support of qualified employees or outside consultants. Institutions that provide retail electronic banking may refer to CEO Memo No. 70, Statement on Retail On-Line Personal Computer Banking, which alerts boards and management to risks and concerns in that area. The memorandum discusses strategic risk, legal/regulatory risk and operational risk as well as security and operations procedures. The memorandum also briefly addresses planning, testing, and monitoring.

As the industry has migrated from direct connect PC banking to Internet banking, the focus of this program (341) is on Internet banking or related activity that involves sending or receiving data using the Internet.

Internet Banking

Internet banking refers to the systems that enable financial institution customers to access accounts and general information on an institution's products and services through a PC or other intelligent device (for example, Internet-enabled wireless phones) in communication with a financial institution's Internet website.

An **Informational Website** provides general information about the financial institution's products and services, and is usually located on a separate server. Informational websites often highlight deposit and loan programs, list branch locations and hours, and provide "email" addresses for customers or the public to contact the thrift. Some informational web sites provide links to other web sites deemed of interest to their community.

For OTS's regulatory purposes, a **Transactional Website** is defined as one that allows customers to do one or more of the following activities:

- Access an account
- Obtain an account balance
- Transfer funds
- Process bill payments
- Open an account
- Apply for or obtain a loan

- Purchase other authorized products or services.

An **Internet-only Bank** represents a special case where the thrift's business strategy rejects the traditional bricks and mortar approach to banking. All or almost all transactions are conducted via the Internet or other electronic networks such at ATMs.

GRAMM-LEACH-BLILEY ACT, PROTECTION OF CUSTOMER INFORMATION

Section V of the Gramm-Leach-Bliley Act of 1999 governs privacy in the context of financial institutions. Subtitle A of that section, titled Disclosure of Nonpublic Personal Information, includes a "Privacy Obligation Policy" and addresses "Financial Institution Safeguards." More specifically, Section 501(a) states, "it is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic information." Section 501(b) directs federal banking agencies such as OTS to "establish appropriate standards for the financial institutions subject to their jurisdictions relating to administrative, technical, and physical safeguards–

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to use of such records or information which could result in substantial harm or inconvenience to any customer."

On February 1, 2001, OTS amended 12 CFR Part 570 Appendix B in order to establish the standards required by Section V of the Gramm-Leach-Bliley Act. Appendix B to Part 570 outlines the Agency's expectations for the creation, implementation, and maintenance of an information security program. This program must include administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. The guidelines describe the oversight role of the board of directors in this process and management's continuing duty to evaluate and report to the board on the overall status of this program.

The four steps in this process require an institution to:

- Identify and assess the risks that may threaten customer information.
- Develop a written plan containing policies and procedures to manage and control these risks.
- Implement and test the plan.
- Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.

The guidelines also set forth an institution's responsibility for overseeing outsourcing arrangements.

OTS examination procedures include review activities to determine an institution's level of compliance with the recently enacted regulatory guidelines.

TECHNOLOGY RISK CONTROL ACTIVITIES

The level of technical knowledge required by boards of directors and senior managers varies depending on the size and nature of its operations, and by the degree of complexities within its technology environment. Nonetheless, 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.

Institutions must establish and maintain adequate functional control systems so management can identify, measure, monitor, and control information technology risks that could adversely affect performance or pose safety and soundness concerns. Similar to basic internal controls, institutions should design technology risk controls

to prevent errors and problems that realistically can be prevented and to promptly detect and address those problems that do occur.

Risks, previously alluded to, may be grouped as following:

- Information Integrity Risk
- Business Continuity Risk
- Vendor Management Risk.

Although the volume and mix of risks will vary depending on the institution's technology environment, each of these types of risk is present at all thrifts. The board of directors and senior management must take steps to prevent, to the extent feasible, the exploitation of any of these risks and to quickly detect and resolve weaknesses and breaches.

Management Oversight

In addition to control activities already discussed, management and board of director oversight responsibilities includes:

- Planning for use of information technology.
- Establishing general control systems.
- Verifying (or auditing) those controls.
- Educating and supporting information technology users, including both staff and customers.

Planning and Implementing Information Technology

Technology is ever changing. From time to time, management will determine to upgrade various parts of its technology environment. This may entail adopting new technologies; upgrading hardware or software; or converting its "environment" (e.g., outsourcing systems previously operated internally or vice versa, or switching from one service provider to another).

Institutions should have an information technology plan that establishes the framework for the deployment and operation of technology. Management should update the plan annually to coordinate technology initiatives and activities to the business planning process. Technologies in place should be subject to periodic review to evaluate performance against current strategic plans and objectives, technological developments, and operating policies and procedures.

The substance and form of any formal plan will vary significantly, depending on the complexity of the institution's information systems and technology. The key element for you to consider is whether the information plan meets the institution's needs.

Management should also ensure that appropriate resources, including the correct mix of staff and a realistic amount of time, are brought to bear on program development or upgrade. A common misunderstanding is that limitations of the computer systems inhibit the development of high quality management information systems. In reality, management has sufficient flexibility under most computer systems to design a management information system that meets the needs of the institution. Therefore, business managers should play a significant role in the development and ongoing assessment of information systems.

General Controls

An institution should require additional data controls for technology that is used to process information. At a minimum, these data input and output controls should provide for accurate data preparation before data input procedures, and segregation of duties between the input of information and the review of that information after it is processed. Such controls generally require the reviewer to reconcile the processed information. In situations involving large-dollar transactions, institutions should require that certain functions be performed under dual control. Management should establish appropriate controls in the early stages of development and deployment and the institution's operating policies and procedures should describe them in detail.

Certain types of input data do not readily lend themselves to robust verification for accuracy and completeness by means of automated edits. Common examples are data from mortgage loan notes, new-account input forms, and PC-prepared spreadsheets. However, verification procedures

may still be warranted, depending on the sensitivity or significance of the data or resulting output. Verification could consist of manually comparing the system output with the source document, or reviewing the data for reasonableness.

Information Integrity Risk

Information is one of an institution's most treasured intangible assets. A major performance factor for institutions is their ability to manage, safeguard, and optimize the use of customer and corporate data.

Information must be:

- Available
- Accurate
- Complete
- Valid
- Secure.

Information integrity concerns are sometimes expressed in the following terms:

Transactional Risk: This is the risk that weaknesses will cause errors to occur in transactions or will prevent a thrift from completing a transaction (or delivering products or services). Individuals may exploit weaknesses to perpetrate fraud via unauthorized transactions.

Reputational Risk: This is the risk that real and perceived errors and lapses in information technology compromise the customer's trust in the accuracy of their account records or the thrift's ability to safeguard the confidentiality of those records.

Compliance Risk: This is the risk that information technology weaknesses will manifest themselves in errors and omissions that cause the institution to be out-of-compliance with laws and regulations.

The weaknesses may or may not be strictly technological. For example, an interest rate risk model might create invalid results due to either faulty programming or inappropriate assumptions. Inaccurate information leads to bad management decisions. Similarly, individuals who perpetrate fraud through technological tools sometimes also employ simple deception – also known as social engineering – to gain passwords from unsuspecting employees.

To combat information integrity risk, the institution should have an active corporate information security program that delineates policy, standards, and management responsibilities. In addition to the policy statement, the program should provide for incident response to security exceptions (for example, employee violations and external unauthorized access attempts), security awareness, and training.

To maintain information integrity and confidentiality, management should establish and enforce controls that safeguard information from unauthorized access and use of data, provide for timely detection and correction of erroneous transactions, and provide for complete audit trails of transaction activity. Management should develop methods to maintain confidentiality, ensure the intended person receives accurate information, and prevent eavesdropping by others. In addition, both the sender and the receiver in a transaction should create undeniable proof of participation.

The scope of information security should address all of the institution's information technology activities, including personal computer activities, Internet-based electronic banking services, and processing by the institution's information service providers.

Effective security does not rely on one solution. Management should use several types of controls to manage information integrity risk:

- User-ID controls.
- Password controls.
- System log-on and log-off controls.
- Virus protection controls.
- Other controls to limit "powerful user" access.
- In some situations the institution will also need to use firewalls and encryption.

User-ID controls, along with password controls, are intended to restrict system access and promote user accountability. For detailed guidance, see CEO Memo 143, Authentication in an Electronic Banking Environment.

User-ID controls include the following:

- Approval: Management-level staff should approve the issuance of user IDs.
- Uniqueness: Each user ID should be identified with only one user (sharing of user IDs should be prohibited).
- Number of IDs per User: In general, each user should only have one user ID, to promote activity monitoring efficiency and employee accountability. Multiple user IDs are sometimes justified (for example, for technical support reasons), but related approval and monitoring controls should be in place.
- Expired or Discontinued Use: User IDs of terminated employees or expired authorizations should be disabled immediately and deleted from the system based on institution policy.

Password controls include the following:

- Length: Experts recommend a minimum of six characters for passwords.
- Composition: Passwords may be alphabetic, alphanumeric, or other. Many experts recommend alphanumeric passwords and avoiding common words like "password" and the names of professional sports teams. Note, however, that complicated passwords may cause users to write them down, especially if the employee needs several passwords to access different systems or applications, and thus compromise the password's confidentiality.
- Expiration: Users should change passwords on a regular basis. The more sensitive the system being protected by the password, the more often the password should be changed. Highly sensitive systems should require password changes at least every 90 days.
- Reuse: The institution should restrict reuse of previous passwords (for example, disallow reuse of the last five passwords used).
- Suppression: All systems should suppress the display of user passwords in any form.
- Encryption: The institution should ensure encryption of password files (the vendor usually encrypts password files for outsourced systems).

Maintenance procedures should ensure that only the user has knowledge of his or her password. Procedures should allow users to change their own passwords.

Access to sensitive data or powerful processing capabilities should require the use of a password. Institution management should promptly reverse temporary privileges, for example, additional access given to an "acting" teller supervisor or branch manager, when no longer needed.

System log-on and log-off controls should limit the number of unsuccessful log-on attempts a user can make. An added enhancement would be to notify the user, upon successful log-on, of unsuccessful attempts since the last log-on interval. PCs and other terminals should automatically log off after a period of inactivity.

Virus-protection controls include policies and software. Policies should restrict employees from importing software from high-risk sources, such as bulletin boards or informally obtained floppy disks.

The institution should install virus-protection software on all PCs and servers. Such software should be updated regularly to protect against new viruses.

The institution should establish **controls to limit powerful user access to system resources**. For example, the institution should appropriately limit "Security Administrator" access, usually to no more than two persons, and the Security Administrator should not have access to customer records.

User Access

Authorized managers grant employees access assignments, which are information retrieval and transaction-processing capabilities. Authorized managers may also grant access to nonemployees

such as consultants, vendor systems-support personnel, and others. For purposes of these procedures, "users" are employees and nonemployees who have authorized system access.

For outsourced systems, service providers may set up generic access assignments for various banking job categories in their access control software. In many cases, thrifts accept and use the vendor-provided access assignments without reviewing or questioning them. This practice increases the risk of inappropriate user access assignments, which in turn weakens controls over user access to sensitive data fields and powerful transaction processing capabilities.

To help ensure that user access assignments are appropriate, institution managers should:

- Identify the system's sensitive customer-record fields (such as account activity status, social security number, and mother's maiden name) and powerful transaction processing features (such as account-linking capabilities and the ability to increase overdraft limits).
- Assign job responsibilities that provide for proper segregation of duties and dual control over sensitive fields and transactions. Institutions should require dual control when using the system's "supervisory override" capability (for example, when approving a transaction keyed-in by a supervisor).
- Assign user information retrieval and transaction processing capabilities according to employees' defined job responsibilities. This step produces user "access profiles."
- Authorize and forward the access profiles to the information security officer for implementation in the system.

If you find any inappropriate user access assignments, determine if the condition was caused by either of the following:

- Control deficiencies in the granting of user access assignments.
- Deficiencies in the system's security controls (system rules or software).

Common deficiencies in security software controls include:

- Deficiencies in implementing certain security software rules. A common example is the inappropriate grouping ("bundling") of transactions by information security officers who maintain the security software. In such cases, large numbers of transaction screens are inappropriately bundled to ease the burden of maintaining security access rules. However, bundling gives many users more system access than required by their job responsibilities.
- Deficiencies in the use of the system's supervisory override feature. In such cases, the dual control (supervisory override) capability of the software has not been properly invoked over certain sensitive fields (such as the dormant-account status field) or powerful transactions (such as the ability to increase an overdraft limit).
- Inherent security software deficiencies. For example, the security software cannot restrict access to certain fields within a record. That is, a user granted access to a record could view or update any field in the record. To alleviate this problem, some companies create additional programs to enhance the capabilities of the basic security software.

Management should determine the frequency of user access assignment reviews. These reviews should be performed at least annually. Management should document these reviews to evidence the performance of the review and approval of changes made.

Firewalls

Firewalls are a combination of hardware and software placed between two networks through which all traffic must pass, regardless of the direction of flow. They provide a gateway to guard against unauthorized individuals gaining access to an institution's network. Institutions should consider firewalls for any system connected to an outside network.

Nonetheless, a firewall does not ensure that a system is impenetrable. Firewalls must be configured for specific operating environments and the insti-

tution must review and update firewall rules regularly to ensure their effectiveness.

Encryption

Encryption is the scrambling of data so that it cannot be read without the proper codes for unscrambling the data. Confidential or sensitive data should always be encrypted when being sent over the Internet and the sender and receiver of the data are not behind the same firewall. This includes email containing confidential and/or sensitive information as well as Internet Banking transactions.

Management should perform a risk assessment to identify types of sensitive data requiring protection and determine the type and strength of encryption to use for various protected communications. The assessment should include databases and password files.

Other Controls

Other information controls that an institution may use to safeguard information integrity include:

- Secure data storage (sensitive data is encrypted; access is stringently controlled).
- Acknowledgement practices (batch totals, sequential numbering and one-for-one checking against a control file can be used to verify that a transaction is complete or has not been interrupted).
- Modem sweeps (efforts to locate and remove unauthorized modems).
- Physical controls (secure storage of hard copies of sensitive data; locks, alarms, etc.).
- Audit procedures (discussed later in this section).

In sum, management should periodically perform a thorough update of its information integrity risk profile and select the appropriate mix of controls to monitor and manage that risk.

Business Continuity Risk

Financial institutions need to be prepared to resume operations as quickly and efficiently as possible after a disaster or other adverse incident. In an Internet environment, these threats may include the loss of Internet access by the institution or loss of access to the institution via the Internet by its customers.

Business continuity risk for an institution relying on one or more service providers includes the risk that it will not be adequately prepared to execute its disaster recovery responsibilities in the event of a disaster affecting the service provider, thereby delaying complete recovery of the institution's financial records. (*Note*: The risks associated with routine service provider system outages are generally low and are not addressed in this handbook section.)

In the context of internally operated systems, business continuity risk is the possibility that the institution will not be adequately prepared to promptly recover from a disaster affecting the computer hardware and software it owns and operates, resulting in significant losses for the institution.

An institution-wide contingency plan provides for timely business continuity if there is disruption to the institution's information technology. Contingency planning, also known as business resumption planning, is a process of reviewing an institution's departments or functions and assessing each area's importance and risks to the viability of the organization. Institution management should establish and maintain disaster recovery plans that address all of its mission-critical systems whether those are operated internally or outsourced. Overall, the extent of a preparedness plan will depend upon the level and complexity of information technology and the institution's available resources.

Management should establish requirements for all operating departments to establish disaster recovery plans for their respective areas of activity. The policy may describe the required components of an acceptable disaster recovery plan (for example, individual responsibilities, resources to be recovered, backup location, and time-line for recovery).

The contingency plan should cover the following areas:

- Define the roles and responsibilities for each team member in the event of a problem situation.
- Identify the risks posed by each system deployed.
- Detail strategies and procedures for recovery.
- Establish criteria for testing and maintenance of plan.
- Identify the principal departments, resources, activities, and constituencies potentially affected by a problem.
- Assess the response capability of key disaster recovery service.

Management should formally appoint and empower individual(s) with the latitude and authority to respond during an incident.

A full understanding of the recovery time line is essential. Full recovery, for example, is usually not achieved when the affected system(s) come "back up" or "back on-line." The institution may have to correct transactions that were in process when the disaster or other disruptive event occurred. In some cases, the institution may have to track down and re-enter the entire day's worth of business.

Management should periodically test and update the contingency plan as needed. Management may accomplish this testing through walk-throughs, tabletop simulations, or other exercises.

OTS's CEO Memorandum No. 72 forwarded the "Interagency Policy on Corporate Business Resumption and Contingency Planning." This package lists a 10-step process that institutions may find helpful in developing contingency plans. The FFIEC IS Examination Handbook (1996; Chapter 10) also discusses contingency planning.

Although management is responsible for institution-wide contingency planning, they should consider different factors depending on whether a particular system is outsourced or internally operated.

Outsourced Systems

Disaster recovery plans for outsourced systems should provide for the following:

- Recovery of lost data for re-submission to the service provider (i.e., day-of-disaster online input).
- Management-approved timeline for completion of recovery.

It is the service provider's responsibility to provide a recovery plan for its computer processing capabilities in the event of a disaster affecting its computer resources. Management should obtain and review (relevant portions of the) contingency plans of its service provider(s):

- To determine that the institution is reasonably protected.
- To ensure that the institution-wide contingency plan is compatible with its service providers' plans.
- To supplement the external contingency plans with appropriate steps the institution itself should take.

The institution's contingency plans for systems involving service providers should do the following:

- Identify all the categories and sources of data input into the service provider's systems by the thrift. Usually, these items are limited to branch and back-office online terminal input. Other items of input, such as automated teller machine (ATM) transactions, automated clearinghouse (ACH) transactions, and in-clearings ("on us" checks negotiated outside of the institution), are usually the responsibility of vendors that provide the respective processing services.
- Describe the steps required to recover previously input data and prepare them for resubmission when requested by the service provider. (Institution management should realize that if the disaster takes place on a business day, online data entered on that day will not have been backed up offsite and will likely be lost.)

- Identify the persons or teams responsible for executing the recovery steps.
- Provide a management-approved time line showing key points, from the point of receipt of notification that the service provider has experienced a disaster to the completion of the preparation of input for resubmission.

Internally Operated Systems

The institution needs additional disaster recovery steps for internally operated systems, especially in the area of backup. The plans should provide for the recovery of key resources, including the infrastructure (computer and operating system software), application software, and data (previously backed up data and day-of-disaster data), as well as, one or more alternate work areas/locations.

Disaster recovery plans for internally operated systems should provide for the following:

- Recovery of lost data (for example, day-of-disaster online input).
- Replacement of damaged resources (such as hardware and software.
- An alternate processing location.
- A management-approved time line for completion of recovery.
- Testing and periodic updating of the plans.

"Recovery" is defined as the point at which application system records (for example, customer balances) have been brought to current status. The recovery time line should provide a breakdown of the various phases of recovery and corresponding elapsed time for each phase of the recovery process.

The institution should periodically copy and store certain data and software components of a system at a prudently distant or remote location to facilitate recovery efforts in the event of a disaster. The institution should perform periodic tests, and resolve within an appropriate time period, any problems the tests reveal. In particular, the tests should verify that the backup files are readable, that is, not corrupted by a record-writing problem. Management should document backup procedures and keep a current inventory of files maintained at the backup site(s).

Vendor Management Risk

Vendor management risk is the risk that the service provider will not perform the contract terms and conditions as specified, causing undesirable consequences for the institution's operations.

When employing the services of an outside service provider or software vendor, management should carefully review proposed service contracts or agreements or renewals thereof to minimize the institution's exposure to risk. Legal counsel should review the draft contract to determine if the interests of the institution are adequately protected.

Before entering into contracts, management should assess and review the following factors:

- Alternate vendors and related costs.
- Financial stability of the vendor.
- Capacity of vendor to stay current with industry developments.
- Requirements for contract termination.
- Contract provisions allowing examination of the vendor.

For detailed guidance, see CEO Memo 133, which details the FFIEC standards for Risk Management of Outsourced Technology Services, and TB 46, Contracting for Data Processing Services and Systems.

After signing a contract for services, management should maintain close oversight of the institution's relationship with the vendor. The institution should establish a contract administration process to ensure that the vendor fulfills its contractual obligations.

Most IT-related contracts specify performance measures for the products or services provided by the vendor. Two common and important measures are online "up time" and "terminal response time." These performance measures generally

have a high impact on the institution's business processes, customers, and employees.

Up time usually refers to the hours and days that online services will be available to the institution. For IT-related contracts, these hours are often the institution's branch operations hours plus two or three additional hours daily. IT contracts should stipulate the vendor's commitment to achieve a high, ongoing level of performance (for example, "99% up time").

Terminal response time usually refers to the standard elapsed time between a user request (for example, the moment when the user presses the Enter Key) and the delivery of information to the user's terminal screen. Current response time standards range from three to five seconds.

In addition, contracts often specify nonproduction-related "deliverables" (products or services) that may enhance the value of the contract for the client. Deliverables may include:

- Commitments to provide the institution with system performance reports.
- Audited financial information.
- Summaries of disaster recovery test results.
- Third-party operations audit reports.
- Other useful materials.

Management should monitor vendor performance. Performance level reports supplied by the service providers should be verified, at least occasionally. Receipt of special services should be verified and payment approved by the business unit receiving those services or the unit monitoring vendor performance. Delivery of nonproduction deliverables should also be monitored. Senior management should be informed promptly of significant deficiencies in vendor performance.

Audit

Institution management is responsible for design and maintenance of a sound system of internal controls that include information technology. The scope of the examiner's assessment of technology risk controls will vary depending on adequacy of the audit function to test and report on those controls. How formal the audit plan is and whether audit work is conducted internally or by external auditors will depend on a number of factors including the institution's size, operations, and technology environment. However, management must ensure that qualified independent (internal and/or external) individuals periodically assess basic technology controls.

The audit plan should provide for review of information technology risks in operations and management activities. This is consistent with an institution's priority to ensure the accurate processing of information, privacy of financial and customer records, and continuation of service in case of business interruptions. In developing audit programs, the institution must consider the full scope of each application to protect financial and information assets, system reliability, and user confidence.

The audit function should cover the flow of critical data through interrelated systems and should generally include the following:

- Tests of balancing procedures of automated applications, including the disposition of rejected and unposted items.
- Periodic samples of customer record files (master files) to verify them against source documents for accuracy and authorization.
- Spot-checks of computer calculations, such as interest on deposits, loans, securities, ARM calculations, service charges, and past-due loans.

Some of these audit functions will not be conducted separately as a "technology" audit but may be incorporated into audits of specific departments or lines of business.

Thrift clients of service providers should obtain "third-party reviews" and take appropriate action in response to control considerations or weaknesses addressed therein. A "third-party review" is a type of independent audit designed to meet the audit needs of financial institutions without overburdening the service provider. That is, without this vehicle a service provider that processes work for several financial institutions could be subject to redundant audits by audit firms for each

of its clients. A qualified auditor who is independent of both the service provider and the serviced institutions conducts the third-party review.

The scope of the audit should be detailed enough to satisfy the audit objectives of the serviced institutions and the servicer. The American Institute of Certified Public Accountants (AICPA) Statement of Auditing Standards (SAS) Number 70 provides guidance for external auditors auditing the servicer as well as for those auditing its financial institution clients. In general, the third-party review audits should determine the adequacy of controls in all areas of the data center, including computer operations, systems and programming, and input/output controls.

Many of the controls that the third-party auditor is to check at the service provider have companion pieces at the individual financial institution. In the third-party review report the auditor typically will address corresponding controls, sometimes known as "client control considerations" that should be maintained at the thrift institution. OTS and FFIEC reports covering service providers may also contain client control consideration. You should review these reports as part of the initial assessment of the institution's IT environment.

Training

Institutions must educate and support customers and staff to achieve user acceptance of and confidence in information technologies. Institutions should provide training so participants properly use applications and respond to problem situations. If an institution fails to provide reasonable training and support for customers and staff, the users' commitment to the system is weakened, administrative expenses increase, and avoidable errors occur. These deficiencies raise the risk of data integrity problems, complaints, and possible legal actions. Risk also increases when an institution fails to educate users on proper security precautions such as locking personal computers and confidentiality of passwords.

Support staff, such as help-line or customer service representatives, should be kept informed of changes and updates to systems. They should be trained on how to execute disaster recovery plans. Management should also provide backup training for key job functions so that human emergencies will not disrupt service.

Internet Activities

The information integrity, business continuity, vendor management, and the management oversight control activities discussed thus far in this chapter pertain to all types of information technologies including Internet activities. This section discusses risks and controls specific to Internet banking and other Internet activities.

Internet Banking

The level of risk posed by Internet banking depends in part on whether the web site is informational or transactional, and if the latter, the nature of the transactions the customer can effect. Informational or information-only web sites are less risky, but not without their vulnerabilities. The web site, for example, may be vulnerable to alteration, so management should establish controls to prevent unauthorized access.

Configurations that provide for electronic mail between the thrift and its customers require additional controls, such as encryption, to protect the confidentiality of customer's accounts and other sensitive data. Customers should be forewarned about including sensitive data such as account numbers in unprotected emails to the institution. Customer passwords rules should be structured to minimize the potential for unauthorized access. For example, institutions should not use readily available customer information for the initial default password, such as, social security number, customer initials, etc. Configurations that permit transactions, including balance/account inquiries, require yet more controls.

OTS-regulated institutions intending to establish a transactional web site must file a notice with OTS at least 30 days in advance of the site opening for business. If an institution implemented a transactional web site since the previous examination, examiners should determine that the institution filed a notice with the appropriate OTS regional office. Examiners should contact the regional office to determine if there were any issues that require a follow-up review.

In planning a transactional web site, it is important to consider the implications on the long-term goals and strategy of the institution and to have input from all of the parties impacted, including managers from both the business and technology sides of the organization, other internal users, auditors, and customers. Planning should begin with a thorough review of objectives to achieve and areas of risk associated with the new activity.

Financial institutions often contract with outside providers to help plan, implement, and maintain Internet banking services. If this is the approach used, institutions should exercise care in selecting a service provider. Also, institution management should give someone in the organization responsibility for monitoring and overseeing their performance on an ongoing basis. In this regard, it is crucial to negotiate a contract that clearly addresses both parties' rights and responsibilities.

Security and internal control are major concerns. Data encryption and digital certificates issued by a reliable certificate authority can be used to protect data and verify the identity of parties communicating online. See CEO Memo 143, Authentication in an Electronic Banking Environment for more detail. An array of firewalls and intrusion detection systems are available to help protect data from theft or alteration. It is important to recognize, however, that those systems do not provide complete protection from attack, and all must be continually monitored and maintained. It is also important to augment electronic security measures with adequate physical security and procedural controls. When adding a transactional web site, institutions need to review and update access to PCs and data, power protection, back-up files, physical locks, security guards, and other common security measures.

Institutions should anticipate the consequences of high demand for electronic services or interruption of service. Institutions should update contingency and recovery plans to address the new activities.

Before opening the transactional web site for use by customers, institutions must update and approve policies and procedures, train employees, and thoroughly test the systems. A plan for periodic risk assessments and audit review should also be in place. Institutions should schedule periodic testing by independent experts in computer security issues, and obtain and review such tests that are conducted for the institution's service providers.

Consumer Compliance and Privacy Issues in Internet Banking

The institution must address consumer compliance and privacy issues in the context of online business. Compliance and legal staffs should review and update procedures for information posted to the web site and all types of transactions to be conducted online. CEO Memorandum No. 90, dated July 23, 1998, regarding Interagency Guidance on Electronic Financial Services and Consumer Compliance may be helpful. See § 573 of the OTS Regulations regarding Privacy of Consumer Financial Information.

General Internet Activities

Management should have policies and controls in place to govern the general Internet activities of its employees. These should include:

Software import: Rules designed to minimize risks (viruses, or other damaging program code) associated with the downloading of software over the network or other sources.

Browsing the Internet: Rules should require the browser to be configured to only access the Internet through a designated firewall and restrict the downloading of certain files.

Encryption: Encryption may be needed to protect sensitive information in transit, such as electronic mail messages, a file being downloaded, or information in storage (for example, databases).

EXAMINATION COVERAGE

Examination coverage for technology risk controls is assigned for each thrift OTS regulates. In general, information technology (IT) examiners review technology risk controls at Internet-only thrifts and those institutions that host their own web sites or that otherwise have complex operations and activities or difficult or non-routine situations. Safety and soundness (S&S) examiners review technology risk controls at the remainder.

This remainder actually represents the great majority of thrifts. Most serviced thrifts will have their technology risk controls evaluated at a regular examination by an S&S examiner, but S&S examiners may also examine other thrifts, including some with in-house data centers or mixed environments.

The regional offices will determine when to assign IT examiners by considering the following factors:

- Recent or pending systems conversions.
- Recent or pending mergers and acquisitions.
- Volume and nature of in-house IT operations.
- Existence of novel or complex applications, systems, networks, or equipment.
- Volume and nature of servicing or software from non-examined entities.
- Problems and concerns at previous examinations.

These factors do not automatically require the presence of an IT examiner, but are indications that may warrant further consideration of such. Similarly, the preceding list does not illustrate the universe of situations that may require the involvement of IT examiners. You should consult with the Regional IT Manager on technology concerns that arise during planning, scoping, or conducting an examination. Such consultation helps ensure proper evaluation and consistent regulatory treatment.

The access and speed capabilities can magnify risk in an electronic environment. This is particularly true if risk management control programs are ineffective or if a system is linked to an institution's central operations or databases. In other words, an institution can be exposed to significant risk even if activity volume is nominal. Consult with your Regional IT Manager if you have any questions about technology risk exposure.

Expanded investigation and analysis may be necessary for some situations, especially significant internal control weaknesses. The examiner completing this program, the examiner in charge (EIC), the Regional IT Manager, and other appropriate regional staff should determine what additional procedures are needed, who should perform them, and whether to do them at the current examination or at a future safety and soundness or IT examination.

S&S examiners should review technology risk controls at all thrifts that are not examined by IT examiners. Technology may have a positive or negative effect on customer service and operating efficiencies, depending on what technologies are employed and how. The availability or unavailability of data and its completeness and accuracy affect decisions in every area of operations. The board of directors and management cannot delegate responsibility to service providers, software vendors, or in-house technology staff, but must ensure that adequate controls exist throughout the organization.

The review of technology risk controls is not a stand-alone task completed by just one examiner. Throughout the examination, all examiners assess the quality and reasonableness of data provided by the institution. For example, examiners evaluating asset quality depend on accurate and complete records of originations, delinquencies, and concentrations for just a few examples. Instances of data that appears questionable or inconsistent and instances of weak controls should be pursued and adverse findings should be relayed to the EIC and the examiner completing Program 341.

In addition, examiners should be sensitive to how the adequacy of the institution's management of information technology can impact our evaluation of each of the CAMELS areas. Listed below are examples of various aspects of information technology and how they impact the CAMELS components.

Capital and Earnings: Information technology may have a positive or negative impact on earnings and capital. The outcome is influenced by several factors.

- Appropriate use of technology can help thrifts improve profitability and ultimately build added capital. On the other hand, adverse impacts could take place if technology acquisitions that are not well coordinated fail to achieve business plan requirements.

- Successful information systems conversions result in meeting tangible and intangible benefits. Poorly executed systems conversions can create large quantities of unposted accounting entries. The resources and time needed to research unposted items increase expenses, and delays in clearing the entries may result in increased charge-offs and dissatisfied customers.
- Using outside vendors may reduce the thrift's capital investments, but may also unnecessarily increase annual expenses and reduce control and flexibility over processing. Long duration contracts with vendors pose risks to a thrift's future earnings and overall performance if the contract process is not closely tied to the corporate business planning.
- Appropriate processing controls are needed to ensure proper reporting of the Thrift Financial Report and various SEC filings.

Asset Quality: Institutions use information technology extensively for processing new loan applications, servicing large pools of loans, and monitoring loan portfolios in a competitive marketplace. Other aspects of automation include the real estate appraisals, loan approval processes, and secondary mortgage activities.

Areas involving technology risks may include:

- Decision support software such as credit scoring used to enhance the credit granting process.
- Internet-based delivery channels.

Management: CEOs and boards of directors are increasing their involvement in information technology decisions. Technology touches every aspect of the institution's operations, and impacts earnings, capital, liquidity, and asset quality:

- Risk management processes, for example, vendor management; information security; contingency planning; project management, may be less robust in small institutions.
- Quality of management information systems.
- Other thrift activities such as general ledger reconciliation, system balancing, and clearing of suspense items. These depend on or affect information systems operations. This includes an institution's internal controls.

Liquidity and Sensitivity: Information technology serves a significant role in cash management. Disruptions could impact customers, cause operating losses, cause an increase in borrowings to offset any cash shortfalls, and place a heavy burden on existing staff to correct the problems.

Technology risks are inherent in all of the following:

- Paper-based cash collections, including check processing, lock-box arrangements, and clearing house activities.
- Electronic based cash collections, including electronic funds transfers such as ATM transactions, ACH, wire transfers, and purchases made with credit or debit cards.
- Management decision-support software used to determine thrift's asset liability mix and balance sheet structure.
- Internet-based delivery channels introduce new technology environments with different kinds of risks, including the potential for a more volatile deposit base.

The review of technology risk controls is not confined entirely to Safety and Soundness or Information Technology examinations. Information technology also supports records and activities reviewed during Compliance and Trust examinations. For example, Truth-in-Lending documents disclosing Annual Percentage Rates and Finance charges commonly are prepared by electronic loan documentation programs and trust administration activities are often automated. Incorrect programming or data entry could result in improper disclosures or untimely action. Again, consult with your Regional IT Manager if you have questions about technology risks in these specialty areas.

Finally, where aspects of a thrift's information technology environment are provided or managed by a holding company or other affiliate, you may need to coordinate the review of some controls with another federal banking agency. Nonetheless, while you should avoid duplication of regulatory oversight, the thrift itself must maintain appropri-

ate internal technology risk controls, which you should assess when completing this program.

EXAMINATION PROGRAM

OTS examinations are risk-based and provide for a comprehensive approach to information technology risks. You use a top-down methodology by determining the information technology environments and risks, evaluating management oversight and control activities, and assessing significant unmitigated risks.

The risk-based examination approach relies on audit work and results that match regulatory needs (for example, audit scope, objectives, and evidence and timing of work). One key criterion is whether or not there is evidence of independent testing and reporting on management policies and operating procedures. If there is no audit to rely on, you will need to perform adequate testing to support conclusions.

"Audit" here refers to the type of work being performed, not the job title of the person doing the work. While internal or external (independent) auditors may complete this work, in many situations, other employees may also perform audit work.

Examination Comments and Rating

You should generally incorporate examination findings and conclusions about Technology Risk Controls into the Management section of the safety and soundness report. ***At a minimum, the report should include a brief description of the institution's use of information technology and an overall conclusion as to the adequacy of controls. You should describe significant adverse findings in sufficient detail to identify specific conditions that warrant corrective action by the institution. Carry forward a summary of such findings to the Examination Conclusions and Comments page.***

The strength or weakness of Technology Risk Controls is one of several factors you consider in assigning a rating to the Management component of CAMELS. You should consider all of the following:

- Specific issues in relation to the volume and trends in transactions, dollars, and customers.
- Apparent risk to the institution's financial and informational assets, including customer data regardless of the volume and trends in activity.
- Anticipated growth in volume, whether dollars, transactions, or customers.
- Anticipated expansion of products, services, or platforms.

Generally, if you identify serious deficiencies with the controls, the management rating should reflect such findings.

OTS Information Technology Database System

The OTS Information Technology Database System provides management information on the industry's data processing activities. This database tracks information on each thrift institution's information technology and electronic banking environment. The database also captures information, for example, name, address, and types of services, on the institution's service providers and software vendors.

Data collection and data verification is handled during the regularly scheduled safety and soundness examination or an information technology examination. The data is collected from the PERK. The S&S or IT examiner should review the information for completeness and accuracy and forward it to the regional office for entry into the database.

REFERENCES

Code of Federal Regulations (12 CFR)

§ 555	Electronic Operations
§ 568	Security Devices and Procedures
§ 563.170	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 563.190(c)	Bonds for Directors, Officers, Employees, and Agents

Part 570

Appendix A	Interagency Guidelines Establishing Standards for Safety and Soundness
Appendix A, II. A.	Internal controls and information systems
Appendix A, II. B.	Internal audit system
Appendix B	Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Office of Thrift Supervision Bulletins and Memoranda

TB 11	Interagency Supervisory Policy on Large-Scale Integrated Financial Software Systems (LSIS)
TB 11-1	Purchased Software Evaluation Guidelines
TB 29	End-User Computing
TB 44	Interagency Statement on EDP Service Contracts
TB 46	Contracting for Data Processing Services and Systems
TB 50	Regulatory Review of Certain Third-Party Contracts
TB 59	Interagency Supervisory Statement on EFT Switches and Network Services
CEO Memo 59	Risk Management of Client/Server Systems
CEO Memo 70	On-Line PC Banking
CEO Memo 72	Revised FFIEC Policy Statement: Corporate Business Resumption and Contingency Planning
CEO Memo 77	Interagency Policy Statement on the Internal Audit Function and Its Outsourcing
CEO Memo 109	Transactional Web Sites
CEO Memo 133	Risk Management of Technology Outsourcing
CEO Memo 143	Authentication in an Electronic Banking Environment

Other References

Federal Financial Institutions Examination Council IS Examination Handbook, 1996.

Regulation (E) Electronic Funds Transfers

OTS Web site, Electronic Banking Page, www.ots.treas.gov

Technology Risk Controls Program

Examination Objective

To assess the extent to which management identifies and mitigates the institution's primary information technology (IT) risks.

Examination Procedures

Technology risk controls essentially are internal controls that an institution should build into daily operations. This program complements traditional examination procedures in the evaluation of specific activities, such as lending, deposit-gathering, and nondeposit activities. You may need to contact examiners in other examination areas to comprehensively evaluate an institution's activities. In addition, you should coordinate efforts to review written policies, internal controls, and other related functions.

If you note problems or unusual factors, consider referrals to information systems, compliance, and other examiners (for example, capital markets specialists). You may also consult with the Regional IT Manager whenever you need additional technological information.

Interagency Guidelines Establishing Standards for Safeguarding Customer Information

Procedures in this program provide for the review and evaluation of a financial institution's compliance to guidelines establishing standards for safeguarding customer information that implement sections 501(b) and 505 of the Gramm-Leach-Bliley Act (GLB). The Interagency Guidelines Establishing Standards for Safeguarding Customer Information is in three parts consisting of: I. An introduction that describes the scope of the guidelines. II. Standards for Safeguarding Customer Information. III. Development and Implementation of information security program.

Part I - Scope: The guidelines apply to customer information maintained by or on behalf of entities over which OTS has authority. These entities are savings associations whose deposits are FDIC insured and any subsidiaries of such savings associations, except brokers, dealers, persons providing insurance, investment companies, and investment advisers.

Part II – Standards: (A) The savings association shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the savings association's size and complexity and the nature and scope of its activities. (B) The savings association shall design the information security program to ensure the security and confidentiality of customer information, protect it against anticipated threats, hazards, and unauthorized access that could result in substantial harm or inconvenience to any customer.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Technology Risk Controls Program

Part III – Development and implementation of information security program: Describes the regulatory agencies' expectations for the creation, implementation, and maintenance of an information security program, consisting of the following:

A. Involve the Board of Directors

B. Assess risks to customer information

C. Manage and control the risks

D. Oversee related service provider arrangements

E. Adjust the information security program, as necessary.

F. Provide a written report to the board regarding the status of the program

G. Implement the (GLB guideline) standards by July 1, 2001.

To evaluate management's compliance to the GLB guidelines, we include and identify the guidelines in Level I and II procedures under Audit, Management Oversight, Information Integrity, Business Continuity, and Internet Banking.

Level I

Wkp. Ref.

1. Ascertain the institution's IT environment and risks. Review the following documents:

   - Standard scoping materials (prior ROE, Regulatory Profile, supervisory correspondence).
   - Preliminary Examination Response Kit (PERK 005), including information related to the Information Technology Database (ITD). Review ITD data for completeness and accuracy. Forward a copy to the regional office according to local instructions.
   - Internal or external audit reports, third-party reviews, and client control letters.
   - Examination reports (by OTS or other FFIEC agencies) pertaining to the institution's IT environment (service providers, software vendors and others).

2. Determine if the institution corrected any previous violations and addressed any criticisms.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

3. Gain an understanding of the institution's IT environment and risks, including:

   - Identify mission-critical systems.
   - Develop an understanding of the IT infrastructure, including Local Area Networks (LANS), Wide Area Networks (WANS), and other IT resources.
   - Obtain information on recent, current and planned major IT projects, such as systems conversions, the introduction of a new product, or the introduction or expansion of electronic banking (including websites).

Audit

4. Assess the adequacy of audit coverage of the institution's IT-related risks and management's responsiveness to audit issues.

   - Determine whether IT audit plans, schedules, and/or audits completed since the preceding examination are commensurate with the institution's IT environment and IT-related risks. The institution should regularly schedule evaluations of the information security program. (GLB III-C)
   - If audit plans and schedules are appropriate:
     - — Determine whether audits have been performed according to plan.
     - — Determine whether audits have appropriately addressed the risks identified in this program.
   - Determine whether significant audit concerns are timely reported to senior management and the board of directors.

5. Assess management's overall responsiveness to audit concerns, including the timeliness of corrective action.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

6. Determine whether other examiners identified significant IT-related issues such as deficiencies related to data integrity, computer models, or information security in areas of their review. If so, investigate the underlying cause(s) and implications. Consult with the examiner in charge and, if appropriate, the Regional IT Manager.

If the thrift has well-qualified staff that conduct a thorough audit of technology risk controls (including the assessment of compliance to GLB information security guidelines), and management responds quickly and appropriately to audit and examination issues, you may conclude this Program now or selectively complete other Level I procedures before concluding.

If an internal or external audit covers technology risk controls, but one or more aspect is weak, lacking, or out-of-date, continue within Level I, and select and complete procedures that correspond to the situation at hand.

If there is no independent review of technology risk controls by an internal auditor, external auditor, or another qualified individual, generally you should complete all of the remaining Level I procedures.

If Level I procedures reveal or suggest weaknesses, complete corresponding Level II procedures.

You may also selectively complete Level II procedures to test Level I findings.

Management Oversight

7. Determine whether the institution has an IT plan appropriate to the size and complexity of its technology environment. Determine whether the board approved the plans, and whether the approval process ensures that the IT plan aligns with the business plan.

8. Review minutes of board and management meetings for evidence of involvement in and approval of significant IT matters. Board minutes should reflect the review and approval of the institution's written information security program and continued oversight over the maintenance of the program. (GLB III-A)

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

Information Integrity

9. Review guidance for employees pertaining to the need to protect the integrity and confidentiality of customer and corporate information. Such guidance may describe the employee's responsibilities and consequences of improper actions. It may also give examples of improper activity, such as, the unauthorized disclosure of customer account information.

10. Determine whether an adequately designed information security program has been established for the institution (GLB III-G requires implementation by July 1, 2001). Information security policies, procedures, and standards now in operation provide for the following (GLB III-B and III-C):

    - Implementation and periodic adjustment of a risk assessment process pertaining to customer and corporate information.
    - Controlled assignment of user access to customer information and sensitive corporate data.
    - Monitoring of access to and use of sensitive or powerful system capabilities (such as the ability to override overdraft or check-cashing limits).
    - Internet services access controls.
    - Data input quality controls (for new accounts, the interest rate control file, and spreadsheets).

11. Review a sample of user access profiles for conformance to policies and procedures. Include sample profiles of teller, back-office, and security administrator access for at least one of the institution's primary systems (such as the deposit, mortgage loan, general ledger system, or Fedline).

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

Business Continuity

12. Assess the overall policy for disaster recovery (Business Continuity and Business Resumption) to determine management's requirements for departments or other operating units to establish, maintain, and test plans for their areas.

13. Review the institution's disaster recovery plans for one or more mission- critical systems and determine if the plans provide for the following (GLB III-C):

    - Recovery of lost customer and corporate data.
    - A management-approved time line for completion of recovery.
    - Testing and periodic updating of the plans.

    For internally operated systems selected, also determine if the plans provide for:

    - Replacement of damaged resources (such as hardware and software).
    - An alternate processing location.

Vendor Management

14. Determine if the institution established adequate vendor-related policies. Ensure that the institution exercises appropriate due diligence in managing and monitoring its service providers. Confirm that the thrift maintains effective information security programs to protect customer information.

15. Assess the institution's controls for monitoring its primary service provider's service-level performance.

    - Determine whether the institution periodically verifies the service-level performance reports supplied by the service provider.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

- Determine whether executive management is promptly informed of significant deficiencies in vendor performance.

Internet Banking

Thrift institutions generally outsource the implementation and operation ("hosting") of Web sites to one or more Internet Service Providers (ISPs). We limit the scope of this program to the review of controls thrift management established to minimize the risk of operating within an internet environment. However, hardware and software controls related to operation of the ISP service are not within the scope of this program.

If the institution hosts its own web site (i.e., the thrift operates its own computer and software to support its web site), an IT examiner should assess the associated controls.

16. Assess the institution's Internet-related information security controls.

    - Determine whether the institution is prepared to deal with Internet information security matters through the support and advise of qualified employee(s) or outside consultants.

    - Determine whether the thrift has established policies and standards related to the use of Internet facilities and services by its employees. The policies should indicate the user authorization process, the Internet services allowed, and the need for controls such as authentication, firewalls, and encryption. (GLB III-C)

    - Assess management's process for verifying the adequacy of its Internet service provider's (ISP) information security and transaction verification controls. (GLB III-D)

17. If the institution created a transactional website since the previous exam determine that they provided the notice to OTS as required by CEO memo No. 109. Contact the regional office to determine the need for follow-up to ensure compliance with the requirements set forth in the CEO memo.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

Level II

Management Oversight

18. Assess the adequacy of IT resource acquisition and outsourcing policy and determine whether it covers cost / benefit analysis; vendor selection and due diligence; management approval (authority limits or guidelines); contract execution; and software licensing. (GLB III-D)

19. Assess the appropriate corporate policy (IT or other) covering insurance to determine whether IT insurance coverage is periodically reviewed and approved by senior management.

20. Determine whether management provides the board with report(s) that describe the overall status of the information security program and the institution's compliance with the GLB guidelines. (GLB III-F)

Information Integrity

21. Determine whether the design of the information security program complies with GLB guidelines as regards the scope and standards for safeguarding customer information. (GLB I and II)

22. Evaluate the customer and corporate information risk assessment process. Management should (GLB III-B):

    - Maintain an inventory of all repositories of customer and corporate information. Management should take particular note of non-public customer information and mission-critical corporate information. Repositories include electronic and paper files.

    - Identify threats to the integrity and confidentiality of the information.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

- Assess the sufficiency of policies and procedures intended to control the risks. Management can accomplish assessments through self-inspection, or through independent audits.

- Monitor, evaluate, and adjust the risk assessment, taking into consideration any change in the IT environment or sensitivity of the information.

23. Assess the user-access assignment process. Determine whether institution managers have (GLB III-C):

- Identified the system's sensitive customer-record fields and powerful transactions.

- Assigned job responsibilities that provide for proper segregation of duties and dual control over sensitive fields and powerful transactions.

- Assigned user information retrieval and transaction processing capabilities according to defined job responsibilities.

- Appropriately limited the assignment of highest user access capabilities (for example, Security Administrator).

- Created and authorized the user access profiles for implementation by the information security officer.

24. Perform sampling tests to verify that user-access assignments are in conformance with management-designed user access profiles (or, in the absence of such profiles, that user access assignments are appropriate).

- Obtain printouts of access profiles of selected users from one of the institution's systems. Include a range of users.

- Ascertain if the system access profiles show inconsistencies with management-designed user access profiles or defined job responsibilities.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

- Identify the sensitive data and transaction processing capabilities of selected users and ascertain if their execution is protected by prudent controls.

25. If you find any user access assignments to be inappropriate, determine if the condition was caused by (a) control deficiencies in the granting of user access assignments or (b) deficiencies in the system's security controls (system rules or software).

26. Determine if management periodically reviews and updates user-access assignments. (GLB III-E)

27. Determine if appropriate controls are in place to monitor activities of employees in areas where proper segregation of duties is not feasible, and of other sensitive activities such as the file maintenance of customer records. (GLB III-C)

28. Determine if appropriate user access and monitoring policies and procedures are adequately documented.

29. Evaluate information security policies and standards in effect for (GLB III-C):

- User-ID controls.
- Passwords.
- System log-on and log-off.
- Virus-protection.
- Encryption of sensitive customer or corporate information whether used and stored within the institution or transmitted elsewhere.
- Destruction or disposal of sensitive customer and corporate information to ensure

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

that the information will not be unintentionally made available to unauthorized persons. Proper disposal could include shredding of paper media, deleting, or degaussing (erasing) of data in electronic media, etc.

30. Assess data-input quality controls. Determine whether controls are in place to verify the completeness and accuracy of sensitive input data that are not readily verifiable by the editing capabilities of the automated system.

31. Assess personnel access restrictions at locations containing customer or corporate information, such as buildings, computer facilities, work areas, and records storage facilities. (GLB III-C)

Business Continuity Risk

32. Assess the institution's disaster recovery plans and testing related to outsourced systems. Obtain and review the institution's service provider-related contingency plan to determine if it (GLB III-C):

- Identifies all the categories and sources of data input into the service provider's systems by the thrift.
- Describes the steps required to recover previously input data and prepare them for resubmission when requested by the service provider.
- Identifies the person or teams responsible for executing the recovery steps.
- Provides a management-approved time line for input resubmission.

33. Determine if the institution periodically reviews the plan to help ensure that it is current and effective. (GLB III-E)

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

34. Assess the institution's disaster recovery plans and testing related to internally operated systems. Obtain and review the plan for a selected mission critical system, and determine if the plan provides for (GLB III-C):

    - The recovery of key resources, including the computer, operating system software, application system software and data.
    - An alternate processing site/work area.
    - Staff assignments, contact lists, and other recovery related provisions as indicated in OTS CEO Memo 72.
    - A management-approved recovery time line for the completion of recovery.
    - Storage of backup files at a safe location.
    - Updated inventory of files maintained at backup sites.

35. Determine if the plan is reviewed periodically to help ensure that it is current and effective. (GLB III-E)

36. Determine if there is adequate protection against destruction of institution-maintained customer or corporate information against potential physical hazards such as fire and water damage (GLB III-C).

Vendor Management Risk

37. Evaluate the appropriateness of existing contracts. Determine if contracts adequately define performance measures related to vendor commitments and if contracts include recommended contract provisions such as those in TB 46 and CEO Memo 133. Also, determine if there are contract provisions and oversight mechanisms to protect the security of customer information maintained or processed by the service providers.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

38. Assess the institution's controls for monitoring vendor performance and ascertain whether (GLB III-D):

    - The institution verifies periodic performance level reports supplied by the service provider.
    - The unit that monitors vendor performance verifies and approves vendor charges for routine and special services.
    - The institution adequately monitors delivery of nonproduction deliverables.
    - Senior management is being promptly informed of significant deficiencies in vendor performance.

Internet Banking

Vendor-Related Controls (GLB D)

39. Review documentation of any due diligence review related to the adequacy of prospective ISPs' information security controls. If you identify significant weaknesses, ascertain their status of resolution. Potential areas of weakness are:

    - Authentication controls
    - Firewall controls
    - Encryption controls
    - Intrusion-detection controls
    - Incidence-handling controls.

40. Assess the effectiveness of controls for the ongoing verification of the adequacy of the ISP's information security program.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

41. Assess management's process for verifying the adequacy of its ISP's business continuity plans. Determine whether management has obtained documented assurance from ISPs that customer transactions are adequately backed up to ensure that they are recoverable in the event of a disaster affecting the ISP.

42. Determine if management monitors the results of tests of the ISP's disaster recovery plans.

43. Assess the appropriateness of the terms and conditions of existing ISP contracts.

44. Assess management's process for monitoring ISP service-level performance.

Institution Controls (GLB III-C)

45. Determine if the institution established policies and procedures to deal with its contractual responsibilities related to outsourced services such as Internet banking, customer bill payment, etc. Procedures should be in place to deal with problem transactions for which the institution is responsible and related customer service activities.

46. Assess controls over the institution's web site systems administrators, if any. The number of administrators should be limited and management should review and approve their web site maintenance capabilities.

47. Determine if the institution's firewall control parameters (i.e., "filters") are described in a document that management reviewed and approved.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

Wkp. Ref.

48. Determine if there are modems in PCs or workstations that would allow unauthorized Internet users (e.g., hackers) to circumvent the institution's firewall. If yes, assess existing controls or management's action plan, to mitigate the risk.

Conclusions

49. Summarize findings, obtain management responses, and update programs and the continuing examination file (CEF), if applicable, with any information that will facilitate future examinations. File exception sheets in the general file.

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

Examiner's Summary, Recommendations, and Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #:

INTRODUCTION

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).

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).

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.

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 as-

signed, 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 reconcilement.
- 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.[1]
- 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)).

[1] Industry practice may have moved from the acceptable range of GAAP to outside of the range.

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 manger 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,[2] 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 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,

[2] 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.

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.

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).

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- 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.

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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- 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.)

Examination Field Procedures

9. Perform recommended follow-up for all items as indicated in the regulatory profile and the Audit-Related Report checklist.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

Level II

Examination Field Procedures

14. 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.

15. 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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- Obtain and review loan listings, contracts, and stockholder listings to substantiate representations of independence, if circumstances warrant.
- 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.

16. 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.

17. Meet with the external auditor to discuss significant audit findings.

18. 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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

Comparison of OTS and FDIC Annual External Audit Requirements

	OTS 12 CFR 562.4	FDIC 12 CFR Part 363
Scope	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)] 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)] 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)] 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'] 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']	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)] 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)]

	OTS 12 CFR 562.4	FDIC 12 CFR Part 363
Auditing Standard	Generally accepted auditing standards (GAAS).	GAAS and the standards of section 37 of the Federal Deposit Insurance Act (FDIA). [12 CFR 363.3(a)]
Qualifications for Auditors	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)] For voluntary audits the CPA does not have to be enrolled in a peer review program. [12 CFR 562.4(e)]	CPA who is independent by AICPA and SEC approved peer review program. [12 CFR 363 Appendix (13), (14), and (15)]
Filing and Notice Requirements **a) Savings Association**	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.	When an audit is required the FDIC requires the following reports: • AFS prepared in accordance with generally accepted accounting principles (GAAP). • Audit Opinion on AFS. • Management Report: — Statement of responsibility — Assessment of effectiveness of the internal control structure over financial reporting, and — Assessment of compliance with designated safety and soundness laws and regulations. • Accountant's attestation report on management's assessment of effectiveness of internal control structure. • Any management letter, qualification, or other report(s) issued by the accountant relating to services provided pursuant to 12 CFR Part 363.

	OTS 12 CFR 562.4	FDIC 12 CFR Part 363
Filing and Notice Requirements **a) Savings Association** *(continued)*	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'] 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'] Institutions that obtain voluntary audits are not required to file any reports or notices with the OTS.	
Audit Waivers	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'] 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']	No similar provision.

	OTS 12 CFR 562.4	FDIC 12 CFR Part 363
Filing and Notice Requirements **b) Auditors**	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]
Audit Committee Requirements	None	Must consist of members of the board who are independent of management[1]. [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.
Documentation and Other Considerations for Audit Work Papers	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)]

[1] 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),[1] the institution should maintain effective systems and internal control[2] 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[3] 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'[4] 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.

---

[1] 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.

[2] This Policy Statement provides guidance consistent with the guidance established in the "Interagency Policy Statement on the Internal Audit Function and its Outsourcing."

[3] 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.

[4] Terms defined in Appendix A are italicized the first time they appear in this policy statement.

The adoption of a financial statement audit or other specified type of external auditing program is generally only required in specific circumstances. For example, insured depository institutions covered by Section 36 of the FDI Act (12 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.[5] 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 inde-

[5] 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.

pendent public accountant stating whether the financial reporting process is subject to any material weaknesses.

Both the staff performing an internal audit function and the independent public accountant or other external auditor should have unrestricted access to the board or audit committee without the need for any prior management knowledge or approval. Other duties of an audit committee may include reviewing the independence of the external auditor annually, consulting with management, seeking an opinion on an accounting issue, and overseeing the quarterly regulatory reporting process. The audit committee should report its findings periodically to the full board of directors.

EXTERNAL AUDITING PROGRAMS

Basic Attributes

External auditing programs should provide the board of directors with information about the institution's financial reporting risk areas, e. g., the institution's internal control over financial reporting, the accuracy of its recording of transactions, and the completeness of its financial reports prepared in accordance with GAAP.

The board or audit committee of each institution at least annually should review the risks inherent in its particular activities to determine the scope of its external auditing program. For most institutions, the lending and investment securities activities present the most significant risks that affect financial reporting. Thus, external auditing programs should include specific procedures designed to test at least annually the risks associated with the loan and investment portfolios. This includes testing of internal control over financial reporting, such as management's process to determine the adequacy of the allowance for loan and lease losses and whether this process is based on a comprehensive, adequately documented, and consistently applied analysis of the institution's loan and lease portfolio.

An institution or its subsidiaries may have other significant financial reporting risk areas such as material real estate investments, insurance underwriting or sales activities, securities broker-dealer or similar activities (including securities underwriting and investment advisory services), loan servicing activities, or fiduciary activities. The external auditing program should address these and other activities the board or audit committee determines present significant financial reporting risks to the institution.

Types of External Auditing Programs

The agencies consider an annual audit of an institution's financial statements performed by an independent public accountant to be the preferred type of external auditing program. The agencies also consider an annual examination of the effectiveness of the internal control structure over financial reporting or an audit of an institution's balance sheet, both performed by an independent public accountant, to be acceptable alternative external auditing programs. However, the agencies recognize that some institutions only have agreed-upon procedures/state-required examinations performed annually as their external auditing program. Regardless of the option chosen, the board or audit committee should agree in advance with the external auditor on the objectives and scope of the external auditing program.

FINANCIAL STATEMENT AUDIT BY AN INDEPENDENT PUBLIC ACCOUNTANT. The agencies encourage all institutions to have an external audit performed in accordance with generally accepted auditing standards (GAAS). The audit's scope should be sufficient to enable the auditor to express an opinion on the institution's financial statements taken as a whole.

A financial statement audit provides assurance about the fair presentation of an institution's financial statements. In addition, an audit may provide recommendations for management in carrying out its control responsibilities. For example, an audit may provide management with guidance on establishing or improving accounting and operating policies and recommendations on internal control (including internal auditing programs) necessary to ensure the fair presentation of the financial statements.

REPORTING BY AN INDEPENDENT PUBLIC ACCOUNTANT ON AN INSTITUTION'S INTERNAL CONTROL STRUCTURE OVER FINANCIAL REPORTING. Another external auditing program is an independent public accountant's examination and report on management's assertion on the effectiveness of the institution's internal control over financial reporting. For a smaller institution with less complex operations, this type of engagement is likely to be less costly than an audit of its financial statements or its balance sheet. It would specifically provide recommendations for improving internal control, including suggestions for compensating controls, to mitigate the risks due to staffing and resource limitations.

Such an attestation engagement may be performed for all internal controls relating to the preparation of annual financial statements or specified schedules of the institution's regulatory reports.[6] This type of engagement is performed under generally accepted standards for attestation engagements (GASAE).[7]

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.[8] 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

---

[6] Since the lending and investment securities activities generally present the most significant risks that affect an institution's financial reporting, management's assertion and the accountant's attestation generally should cover those regulatory report schedules. If the institution has trading or off-balance sheet activities that present material financial reporting risks, the board or audit committee should ensure that the regulatory report schedules for those activities also are covered by management's assertion and the accountant's attestation. For banks and savings associations, the lending, investment securities, trading, and off-balance sheet schedules consist of:

Area	Reports of Condition and Income Schedules	Thrift Financial Report Schedules
Loans and Lease Financing Receivables	RC-C, Part I	SC, CF
Past Due and Nonaccrual Loans, Leases, and Other Assets	RC-N	PD
Allowance for Credit Losses	RI-B	SC, VA
Securities	RC-B	SC, SI, CF
Trading Assets and Liabilities	RC-D	SO, SI
Off-Balance Sheet Items	RC-L	SI, CMR

These schedules are not intended to address all possible risks in an institution.

[7] 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.

[8] 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.

the fairness of the institution's financial statements or attest to the effectiveness of the internal control structure over financial reporting. The findings or results of the procedures are usually presented to the board or the audit committee so that they may draw their own conclusions about the quality of the financial reporting or the sufficiency of internal control.

When choosing this type of external auditing program, the board or audit committee is responsible for determining whether these procedures meet the external auditing needs of the institution, considering its size and the nature, scope, and complexity of its business activities. For example, if an institution's external auditing program consists solely of confirmations of deposits and loans, the board or committee should consider expanding the scope of the auditing work performed to include additional procedures to test the institution's high risk areas. Moreover, a financial statement audit, an examination of the effectiveness of the internal control structure over financial reporting, and a balance sheet audit may be accepted in some states and for national banks in lieu of agreed-upon procedures/state-required examinations.

Other Considerations

TIMING. The preferable time to schedule the performance of an external auditing program is as of an institution's fiscal year-end. However, a quarter-end date that coincides with a regulatory report date provides similar benefits. Such an approach allows the institution to incorporate the results of the external auditing program into its regulatory reporting process and, if appropriate, amend the regulatory reports.

EXTERNAL AUDITING STAFF. The agencies encourage an institution to engage an independent public accountant to perform its external auditing program. An independent public accountant provides a nationally recognized standard of knowledge and objectivity by performing engagements under GAAS or GASAE. The firm or independent person selected to conduct an external auditing program and the staff carrying out the work should have experience with financial institution accounting and auditing or similar expertise and should be knowledgeable about relevant laws and regulations.

SPECIAL SITUATIONS

Holding Company Subsidiaries

When an institution is owned by another entity (such as a holding company), it may be appropriate to address the scope of its external audit program in terms of the institution's relationship to the consolidated group. In such cases, if the group's consolidated financial statements for the same year are audited, the agencies generally would not expect the subsidiary of a holding company to obtain a separate audit of its financial statements. Nevertheless, the board of directors or audit committee of the subsidiary may determine that its activities involve significant risks to the subsidiary that are not within the procedural scope of the audit of the financial statements of the consolidated entity. For example, the risks arising from the subsidiary's activities may be immaterial to the financial statements of the consolidated entity, but material to the subsidiary. Under such circumstances, the audit committee or board of the subsidiary should consider strengthening the internal audit coverage of those activities or implementing an appropriate alternative external auditing program.

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.[9] 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:

[9] 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 board of directors or its audit committee adequately reviews and approves external auditing program policies at least annually.
- The external auditing program is conducted by an independent public accountant or other independent auditor and is appropriate for the institution.
- The engagement letter covering external auditing activities is adequate.
- The report prepared by the auditor on the results of the external auditing program adequately explains the auditor's findings.
- The external auditor maintains appropriate independence regarding relationships with the institution under relevant professional standards.
- The board of directors performs due diligence on the relevant experience and competence of the independent auditor and staff carrying out the work (whether or not an independent public accountant is engaged).
- 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[10] 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.[11] 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.

[10] 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.

[11] 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.

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 responsible for monitoring the group. If the institution is a subsidiary of a holding company, the term "appropriate supervisory office" also includes the federal banking agency responsible for supervising the holding company. In addition, if the institution is state-chartered, the term "appropriate supervisory office" includes the appropriate state bank or savings association regulatory authority.

Audit. An examination of the financial statements, accounting records, and other supporting evidence of an institution performed by an independent certified or licensed public accountant in accordance with generally accepted auditing standards (GAAS) and of sufficient scope to enable the independent public accountant to express an opinion on the institution's financial statements as to their presentation in accordance with generally accepted accounting principles (GAAP).

Audit committee. A committee of the board of directors whose members should, to the extent possible, be knowledgeable about accounting and auditing. The committee should be responsible for reviewing and approving the institution's internal and external auditing programs or 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 Cer-

tified 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.

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

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: _____

INTRODUCTION

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.

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 re-

port 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 cosourcing," 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 Thrift Activities Regulatory 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 Systems 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)

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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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

11. 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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

12. 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.

13. Check for progress in correcting any earlier reported areas with significant weakness. Identify the responsible party to make the correction and the time frame.

14. Check the adequacy of information on the audit function available to management and the board of directors or its audit committee.

15. 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.

16. 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 committee. Test for evidence of insider abuse, known or suspected defalcations, known or suspected criminal activity, and questionable transactions with affiliates.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

17. 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.

18. 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit Questionnaire

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.

	Yes	No
1. Has the auditor devised an overall audit plan identifying areas of risk?		
2. Do programs and questionnaires exist for each area?		
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?		
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?		
• Does the arrangement comply with current AICPA guidance?		
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?		
• They did not audit records of the department to which they are assigned or their own work?		
6. Does the internal auditor meet with the directors at least annually to discuss written reports of audit?		
How often? _____		

	Yes	No
7. Do audit programs include tests of physical and accounting controls performed in the following (minimum) areas:		
• Cash?		
• Consigned items and other nonledger control accounts?		
• Investments?		
• Loans?		
• Loans and participations sold and purchased?		
• Allowances for credit losses?		
• Deposits?		
• Confirmation of loans and deposits?		
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?		
• How often? _____		
• Do they make cash counts on a surprise basis?		
2. Do they test bank account reconciliations for accuracy?		
3. Do they test cash receipt procedures?		
4. Do they test cash disbursement procedures?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit Questionnaire

	Yes	No
• Do they review cash control records and trace any apparently large or unusual cash movements to or from a department or branch?.....		
Funds Transfer Activities		
1. Does the internal auditor review the wire transfer function for segregation of duties involving receipt, processing, settlement, accounting, and reconciliation?		
2. Does the internal auditor test staff compliance with credit and personnel procedures, operating instructions, and internal controls?		
3. Does the internal auditor review overnight drafts?.....		
Due From Banks		
1. Does the internal auditor test the bank reconcilement including the Federal Reserve Bank?.....		
• 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 reconcilement?		
2. Does the internal auditor review all returned items for an appropriate period subsequent to the examination date?		
3. Does the internal auditor confirm due from banks?		
4. Does the internal auditor check the accuracy and completeness of reports submitted to the Federal Reserve for calculation of required reserve balances?		

	Yes	No
Consigned Items and Other Nonledger Control Accounts		
1. Does the internal auditor balance and confirm consignment items?.....		
• How often? _____		
• On a surprise basis?.....		
2. Does the internal auditor test income from the sale of consignment items?.....		
3. Does the internal auditor test rental income for safe deposit boxes?		
4. Does the internal auditor check vault entry records for signature(s) of authorized persons?		
5. Does the internal auditor examine safekeeping/custodial accounts or confirm them with an outside custodian?		
6. Does the internal auditor test the completeness of safekeeping/custodial items and records by examining supporting documentation or by confirming with customers?		
7. Does the internal auditor test closed safekeeping/custodial accounts?		
8. Does the internal auditor test fee income for safekeeping/custodial accounts?		
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? ..		
• Does the internal auditor test collection fee income?.....		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit
Questionnaire

	Yes	No
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.?.....		
2. Does the internal auditor examine or confirm all investment securities?.....		
3. Has the internal auditor ascertained that securities transactions are in keeping with stated portfolio objectives?		
Has the internal auditor also:		
• Reviewed the securities dealers with who the institution conducts securities activities?		
• Reviewed objectionable investment portfolio transactions?.....		
4. Does the internal auditor test that all investment securities transactions are authorized?		
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)?.....		
6. Does the internal auditor verify the book and market values of investment securities?		
7. Does the internal auditor reconcile the accrued interest accounts to detail, and check computations of interest income?.....		
8. Does the internal auditor test the gain and loss on investment securities sold during the period?.....		
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?		
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)?.....		
11. Does the internal auditor check for compliance with the FFIEC "Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities?"		
12. Does the internal auditor check for compliance with the repurchase agreement provision of the Government Securities Act for non-dealer entities?.....		
Retail Nondeposit Investment Sales		
1. Does the internal auditor check the monitoring and resolution of customer complaints?		
2. Does the internal auditor test customer accounts for proper disclosures?.....		
3. Does the internal auditor check for conflicts of interest?.....		
4. Does the internal auditor review the saving association's compensation program for retail nondeposit investment product sales?		
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?.....		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

	Yes	No
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?		
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 Retails Sales of Nondeposit Investment Products?"		
Subordinate Organizations and Affiliates		
1. Does the internal auditor review and test the investment in and the transactions with related organizations?		
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?		
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)?		

	Yes	No
2. Does the internal auditor validate the data integrity of significant market, liquidity, and risk management models?		
3. Does the external auditor determine that contract documentation is properly maintained and safeguarded, and ascertain that legal counsel has properly reviewed documents?		
4. Has the external auditor confirmed the effectiveness of internal control systems used for derivatives transaction processing and valuation?		
5. Has the external auditor checked compliance with laws, rules, regulation, proper accounting, and taxation considerations?		
6. Has the internal auditor ascertained the savings association staff performs derivative activities within the guidelines provided by bank policies and procedures?		
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?		
2. Does the internal auditor determine whether compliance with policies and procedures is adequate?		
3. Does the internal auditor test delinquency lists?		
• How often? _____		
4. Does the internal auditor test interest and accrual computations?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit
Questionnaire

	Yes	No
• How often? _____		
5. Does the internal auditor verify loan and escrow (impound) account balances (includeing confirmation procedures)?.....		
• Does the internal auditor physically inspect collateral, if applicable?.....		
• Has the internal auditor tested the pricing of negotiable collateral, if applicable?....		
6. Does the internal auditor examine notes and other legal documentation for authorized approvals and compliance with policies?....		
7. Do the internal auditor's work papers disclose:		
• The number and percent of new loan files examined compared with the total originated during the period?.....		
• The number and percent of files applicable to previous audit periods examined compared with the total number outstanding as of the audit date?		
• The basis used for selection of loan accounts for inspection and the specific documents inspected?.....		
8. Does the internal auditor note all material exceptions?.....		
9. Does the internal auditor determine the adequacy of insurance coverage and ensure that the institution names itself as loss payee?		
10. Does the internal auditor verify the loan-in-process accounts?.....		
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?.....		

	Yes	No
Loans and Participations Sold or Purchased		
1. Do the internal auditor's work papers indicate the extent of audit procedures performed and conclusions reached?.....		
2. Does the internal auditor confirm:		
• Significant balances of loans and participations sold or purchased?		
• Significant terms of purchase or sales agreements?.....		
3. Do the internal auditor's work papers indicate the methods used to determine the adequacy of auditing procedures on loans serviced by others?.....		
4. Do the internal auditor's procedures include, when appropriate, obtaining letters from servicing organizations' auditors confirming the extent of their audit procedures?		
5. For loans purchased, do the internal auditor's procedures verify that:		
• The underwriting meets the institution's underwriting standards?		
• The institution obtains, reviews, and retains all pertinent documents?.....		
Mortgage Banking Activities		
1. Does the internal auditor test book and fair-market values of mortgage servicing assets?		
2. Does the internal auditor verify the appropriateness of hedge accounting?.....		
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?.....		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

	Yes	No
• Did the internal auditor follow up on any exceptions outstanding over 120 days?		
4. Does the internal auditor test impairment analyses?		
5. Does the internal auditor determine the accuracy of financial reporting systems and other management information systems?		
6. Does the internal auditor check compliance with established policies and procedures, accounting procedures, lows, rules, and regulations?		
Leasing Activities		
1. Does the internal auditor confirm leases and related balance sheet accounts?		
2. Does the internal auditor review the leases and other legal documentation?		
3. Does the internal auditor test the computation of depreciation expense, interest expense, or rental income?		
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?		
5. Does the internal auditor determine that account balances accurately reflect any deferred tax liability or asset?		
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?		

	Yes	No
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):		
• Does the internal auditor verify loan balances for the loans charged off since the last audit?		
• Does the internal auditor examine the supporting documentation for loans charged off?		
• Does the internal auditor reconcile loan recovery detail amounts to credit entries in the appropriate general ledger accounts?		
• 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?		
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?		
• Does this methodology comply with OTS policy, GAAP, and industry practice?		
3. Is an adequate record available indicating which assets the internal auditor reviewed for classification and when?		
4. Does the internal auditor consider self-classifications of loans in determining the adequacy of the allowances for credit losses?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit Questionnaire

	Yes	No
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?		
Deposits: Demand, Time Deposit Savings Accounts, and other Transaction Accounts		
1. Does the auditor maintain up-to-date documentation showing savings policies and practices?		
2. Is the extent of the internal auditor's tests to determine compliance with board-approved policies and practices adequate?		
3. Does the internal auditor address the following (minimum) areas for dual control and segregation of duties:		
• Inactive accounts?		
• Closed accounts: Does the internal auditor test closed accounts and determine that they were properly closed?		
• 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?		
• Passbooks and certificates?		
• Certificates of deposit: Does the internal auditor account for numerical sequence of pre-numbered certificates of deposits?		
• Opening accounts?		
• Closing accounts?		
• Loans on deposits?		
• Account transfers?		
• Interest (dividend) computation?		
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?		
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?		
• What basis does the internal auditor use to select accounts to confirm? _____		
• Is it appropriate?		
3. If the internal auditor uses statistical sampling, do the work papers disclose:		
• The method used?		
• A selection system with a random start?		
• The confidence level achieved?		
4. Does the internal auditor report all material exceptions?		
5. Does the internal auditor review overdraft accounts and determine collection potential?		
Official Checks		
1. Does the internal auditor reconcile account balances?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit Questionnaire

	Yes	No
2. Does the internal auditor determine the validity and completeness of outstanding checks?		
3. Does the internal auditor examine documentation supporting paid checks?		
4. Does the internal auditor test certified checks to customers' collected funds balances?		
Other		
1. Does the internal auditor test borrowings for approval and regulatory compliance?		
• How often? _____		
• Does the internal auditor confirm borrowed funds?		
• Does the internal auditor examine supporting legal documents, disclosures, and collateral custody agreements, and determine compliance with applicable laws and regulations?		
• Does the internal auditor review the minutes of the stockholders' and board of directors' meetings for approval of all borrowing requiring such approval?		
• Does the internal auditor verify changes in capital notes outstanding?		
• Does the internal auditor review the accrued interest accounts and test computation of interest expense?		
2. Does the internal auditor review the adequacy of the scope of auditing procedures for Other Liabilities and Deferred Credits?		
• Does the internal auditor confirm balances of "other liability" accounts (including tests for unrecorded liabilities as of a given date)?		
• Does the internal auditor review the operation and use of any "inter-office" account?		
• Does the internal auditor review suspense accounts to determine that appropriate staff clears all items on a timely basis?		
3. Does the internal auditor review whether the scope for auditing real estate owned (REO) accounts is adequate?		
• Does the internal auditor review procedures to ensure that the institution purchases appropriate hazard insurance?		
• Does the internal auditor review current appraisal procedures, market values, and sales prices?		
• Does the internal auditor review foreclosure procedures including whether the institution has proper title?		
• Does the internal auditor verify expenses to maintain properties, and confirm rental income?		
• Does the internal auditor review monthly reconciliations of the properties to he general ledger?		
• Does the internal auditor review REO reports to the board of directors?		
4. Does the internal auditor's scope for auditing fixed assets include the following procedures:		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit
Questionnaire

	Yes	No
• Examining support for additions, sales, and disposals?		
• Reviewing property transactions with "bank-affiliated personnel?"		
• Verifying property balances?		
• Testing computation of depreciation expense?		
• Testing computation of gain or loss on property sales and disposals and tracing sales proceeds to cash receipts records?		
• 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?		
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?		

	Yes	No
Income and Expense		
1. Does the internal auditor's scope adequately address all significant income and expense accounts?		
• Does the internal auditor test income and expenses by examining supporting documentation for authenticity and proper approval?		
• Does the internal auditor test accruals by either recomputing amounts or examining documents supporting such accruals?		
• Test computations for gains and losses on disposals, and for amortizations?		
• Review inter-office transactions and suspense accounts to determine whether all items included were temporary?		
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?		
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?		
3. Does the internal auditor review capital changes?		
Dividends		
1. Does the internal auditor verify computation of dividends paid and/or accrued on stock?		

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Internal Audit Questionnaire

	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?		
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?		
2. Does the internal auditor control or periodically review dormant accounts?		
3. Does the internal auditor review unposted items?		
Payment System Risk		
1. Does the internal auditor test the bank's self-assessment?		
2. Does the internal auditor review the reasonableness of any de minimis cap?		
3. Does the internal auditor ascertain compliance with established bank policy?		
Asset Management		
1. Does the internal auditor test fee income and client reimbursement?		
2. Does the internal auditor examine asset management client contracts?		
3. Does the internal auditor check for compliance with applicable laws, regulations, and rulings?		
4. Does the internal auditor ascertain adherence with established bank policies and procedures?		
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?		

Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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[1] 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).[2] 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 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.

[1] 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.

[2] 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.

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.[3] The board or its audit committee should develop objective performance criteria to evaluate the work of the internal audit function.[4]

[3] 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.

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

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.[5] 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.

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.[6]

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

[5] 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.

[6] 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.)

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 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[7]

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."

[7] The guidance in the preceding section of this policy statement ("The Internal Audit Function") also applies to internal audit outsourcing arrangements.

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;
- 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.[8]

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.[9]

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

[8] 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.

[9] 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.

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 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."[10]

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:[11]

- 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.

[10] 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).

[11] 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

.206 *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?

.207 *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

.208 *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?

.209 *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

.210 *Question* - In providing extended audit services, would the frequency with which a member performs an audit procedure impair the member's independence?

.211 *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]

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: >

		Yes	No
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?	____	____

Cash and Cash Items

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: >

		Yes	No
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.		

_____

Due From Banks

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 reconcilement 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: >

			Yes	No
		Investment Portfolio		
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?		
		_____		
		Demand Deposits		
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: >

			Yes	No
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 escheat 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 escheat 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: >

		Yes	No
57.	List the last audit date for this area.		
	_____		
	Loans		
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		
	_____		
	Wire Transfers		
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: >

		Yes	No
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		
	_____		

INTRODUCTION

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.

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[1] 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.

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 Thrift Activities 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.

[1] 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.

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 re-

cords (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 re-

cords 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[2] 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.
- 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.

[2] Section 563.180(d) treats a savings association and its operating subsidiaries as one unit.

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 Compliance Handbook Section 400, Bank Secrecy Act.

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)

Fraud/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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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.

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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

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

13. Choose a sample of SARs that the institution has filed. Review each sample SAR to determine its accuracy, completeness, timeliness, and propriety.

14. Complete the following procedures if you have identified any instance of suspected criminal misconduct:

    - Immediately notify the EIC and field manager.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- 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.

15. 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.

16. 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.

17. 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:

- Made, or has entered into an agreement to make, any golden parachute or indemnification payments.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

- 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.

18. 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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[1]	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		

General Factors	Indicator: Lower	Indicator: Higher	Comment or Description	Risk Factor
Internal audit department turnover	None or minimal	High		
Policies and procedures	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		
Unusual or lavish fixed assets	None	Boats, aircraft, artwork, condos, etc.		
Internal controls	Sound system of controls	Material control deficiencies; or controls do not apply to top management		
Response of management in providing documents to examiners	Documents provided quickly	Long delays in getting documents		
Transactions with other financial institutions	Appropriate for business activities	Large transactions with small out of state banks		
Board reports	Accurate and complete	Inaccurate; inadequate; incomplete		
Organizational structure	Simple	Overly-complex		
Aggressive accounting practices/tax-motivated behavior	Few	Many		
Regulatory violations	Few	Many		
Criminal Referrals	Few	Many		
Falsified bank records	None	Many		

Lending Factors

Loan documentation	Well-documented loans and credit quality	Poorly documented loans		
Loan performance tracking	Close review of problem credits by management and the board	No (or erroneous) past due or watch list reports		
Borrower financial statements	Borrowers' financial position well documented	No (or unsigned) financial statements		
Loan disbursements	Well documented; approved by an independent officer	Questionable; approved by loan officer		
Corporate loans	Proper endorsements and guarantees	No (or inadequate) endorsements and guarantees		
Resolution of problem loans	Well documented and reasonable	Questionable pay-downs prior to examination or audit		
Overdrafts	Properly approved; reasonable amounts	Large questionable overdrafts		
Refinancing	Well documented; properly approved	Poorly documented; refinanced by a different department		
Nominee loans	No nominee loans	Nominee loans made		
Loan terms	Loan size, rates and maturities appropriate	Loans of unusual size, rates, and maturities		
Evergreen/non-amortizing loans	No evergreen/ nonamortizing loans	Several large evergreen/ nonamortizing loans		
Real property sales history	Well-documented history of sales and ownership	No history of sales or ownership		
Out of territory loans	No out of territory loans	Many out of territory loans		
Brokered loans	No brokered loans	Loans from brokers		
Adequacy of collateral	Loans adequately collateralized when appropriate	Large loans with unusual, questionable, or no collateral		
Collateral sales history	Collateral sales history is reasonable	Frequent sales; flipped collateral		
Loans to directors, officers, and employees	Properly underwritten and reported to the board of directors	Loans to uncreditworthy directors, officers, or employees		

Lending Factors	Indicator: Lower	Indicator: Higher	Comment or Description	Risk Factor
Lending authority	Large approval limits are vested in the board or its committee	Large approval limits given to individuals or to inexperienced or inappropriate employees		
Third-party disbursements	Disbursements made to borrowers	Disbursements made to third parties		
Construction disbursements	Property inspected by independent institution officer prior to disbursement	No or poorly documented inspections; no rotation of inspectors		
Asset performance	Very low percentage of delinquent/nonperform-ing/classified assets	High percentage of delinquent/nonperforming/ classified assets		
Independent loan review function	Effective; independent loan review function	No (or ineffective) loan review		
Speculative, high-risk lending activities	Institution has conservative lending practices	Institution engages in high-risk lending activities		
Predatory lending practices	None	Institution engages in predatory lending practices		

Deposit Factors

Concentrations of deposits	No concentrations of deposits	High concentration of deposits by individuals, firms, or public entities		
Brokered deposits	No brokered deposits	High level of brokered deposits		
Training for all personnel on effective check fraud prevention	Comprehensive training program for all personnel on check fraud prevention	No training on check fraud prevention		
Check cashing guidelines	Comprehensive check cashing guidelines	No check cashing guidelines		
New accounts	Comprehensive guidelines for opening new accounts	No guidelines for opening new accounts		
Signature cards	Signature cards secure, permanent, and updated	No control over signature cards		
Account changes	Account changes require identification and written requests	No controls over account changes		
Dormant accounts	Dormant account activity requires extra approvals or mandatory holds	No controls on dormant accounts		

[1] 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:

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 statue 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 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)(l)(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.

INTRODUCTION

The Office of Thrift Supervision (OTS) uses its statutory authorities to take prompt and vigorous enforcement action when warranted to ensure compliance with laws and regulations and the safety and soundness of savings associations.[1] Proper use of OTS's formal enforcement powers and informal supervisory responses is critical in helping OTS meet its functional responsibilities:

- Ensuring the safety and soundness of the thrift industry.
- Ensuring that all associations and their holding companies comply with laws and regulations.
- Maintaining the soundness of the insurance funds.

OTS uses its enforcement powers primarily to halt unlawful acts or practices and to require corrective action. OTS may take enforcement action against savings associations, savings and loan holding companies, service corporations, operating subsidiaries, other affiliates, or institution-affiliated parties (IAP)[2] to ensure the safety and soundness of savings associations and the thrift industry in general.

The enforcement policies in this handbook section apply to all the parties listed in the paragraph above as well as all examination types.

OTS uses formal and informal enforcement tools to carry out its supervisory and enforcement responsibilities; to address violations of laws and regulations, conditions imposed in writing and written agreements with the agency; and to address unsafe and unsound practices. These tools are the focus of this Handbook section.

SUPERVISORY POLICIES

Selecting the Appropriate Tool

Choosing the appropriate supervisory response involves the careful balancing of factors and the exercise of discretion. Below we list the general considerations for determining whether to use a formal enforcement action or an informal supervisory response:

- The extent of actual or potential damage, harm, or loss to the savings association because of the action or inaction.
- Whether the association or an IAP has repeated the illegal action or unsafe or unsound practice.
- The likelihood that the conduct may occur again.
- The association's record for taking remedial or corrective action in the past.
- The capability, cooperation, integrity, and commitment of the association's management,

[1] These policies and procedures only provide guidance. They are not intended, do not, and may not be relied upon to create rights, substantive or procedural, enforceable at law or in any administrative proceeding.

[2] Institution-affiliated party means:

- Any director, officer, employee, or controlling stockholder (other than a savings and loan holding company) of, or agent for, an insured depository institution.
- Any other person who filed or OTS requires to file a change-in-control notice with OTS under 12 USC § 1817(j).
- Any shareholder (other than a savings and loan holding company), consultant, joint venture partner, or any other person as determined by OTS (by regulation or case-by-case) who participates in the conduct of the affairs of an insured depository institution.
- Any independent contractor (including any attorney, appraiser, or accountant) who knowingly or recklessly participates in any:
  — violation of any law or regulation,
  — breach of fiduciary duty, or
  — unsafe or unsound practice,

  which caused or is likely to cause more than a minimal financial loss to, or have a significant adverse effect on, the insured depository institution. 12 USC § 1813 (u).

board of directors, and ownership to correct identified problems.

- The extent to which the identified problems were preventable and not solely the result of external factors.
- The effect of the illegal, unsafe, or unsound conduct on other financial institutions, depositors, or the public.
- The examination rating of the association.
- Whether the association's condition is improving or deteriorating.
- Whether another government agency's or private party's litigation or actions will achieve OTS objectives.
- The presence of unique circumstances.
- The supervisory goal OTS wants to achieve.

The last factor, the supervisory goal, is especially important. For example, a Cease and Desist (C&D) order may require affirmative corrective actions, including the payment of restitution or reimbursement to an institution, but cannot require the removal or prohibition of an individual from participating in the institution's affairs. That remedy requires issuance of a Removal and Prohibition (R&P) order, based on the statutory elements in 12 USC § 1818(e).

OTS considers the following items before determining whether an association's problems are serious enough to warrant a formal enforcement action or whether an informal action, such as a board of directors' resolution, supervisory meeting, or correspondence can adequately address the association's problems:

- An analysis of the facts.
- An assessment of the seriousness of the problem.
- The association's supervisory history.
- The quality of management involved.
- The results of any meeting with the board of directors.
- An evaluation of whether management will take appropriate corrective action.
- An assessment of the potential harm to the association if the association does not take corrective action.

Policy on Enforcement Actions

When to Take Formal Enforcement Action

For serious problems or deficiencies, formal enforcement action may be the appropriate initial action. There is a strong presumption that OTS will take prompt formal enforcement action against any association with serious problems regardless of examination ratings or capital levels. Examples of when OTS will consider taking formal enforcement action include, but are not limited to, one or more of the following situations:

- The association's records, systems, controls, policies, or internal audit program exhibit significant problems or weaknesses.
- There is serious insider abuse.
- There are substantial violations of law or regulations.
- There is material noncompliance despite prior commitments to take corrective actions. (If the association does not comply with an informal enforcement action within a reasonable time, absent strong justification, a formal action is strongly indicated.)
- The board does not take corrective action.
- Informal actions are insufficient.
- The association does not maintain satisfactory books and records or provide OTS or other regulatory authorities with prompt and complete access to books and records.

4- and 5-Rated Associations

There is a strong presumption that savings associations with a composite rating of 4 or 5 for the latest safety and soundness, compliance, trust, or information technology examination, or unsatisfactory rating for the latest holding company examination warrant formal enforcement action. Because a 4- or 5-rated association is more likely to fail, a formal OTS corrective action is presumed necessary.

For 4- and 5-rated associations that are currently subject to informal enforcement actions, OTS will consider imposing a formal enforcement action if the most recent examination reaffirms or reclassifies the association's composite rating.

3-Rated Associations

There is a presumption that savings associations with a composite rating of 3 for the latest safety and soundness, compliance, trust, or information technology examination warrant formal enforcement action under any of the following circumstances:

- Management is weak.
- There is uncertainty as to whether management and the board have the ability or willingness to take appropriate corrective measures.
- Conditions are rapidly deteriorating.
- A 3-rating continues for two consecutive examinations following the thrift entering into the informal enforcement action, unless the thrift complies with the informal enforcement action and no new grounds exist for taking a formal action.

OTS may consider issuing an informal enforcement action for a 3-rated association with strong management and a generally positive assessment if circumstances suggest that remedial measures are immediately forthcoming. The capability, cooperation, integrity, and commitment of management, board, and owners are important considerations in choosing the appropriate actions.

Holding Companies

There is a strong presumption that holding company enterprises with an unsatisfactory rating warrant formal enforcement action. Other factors that might influence OTS's decision to take enforcement action against a holding company and its subsidiaries include:

- Information or referrals from another financial regulator, including a functional regulator such as the SEC, about the holding company.
- Significance of the problems or weaknesses.
- The potential threat that holding company problems might pose a reputation risk for the savings association.
- Severity of the effect the holding company enterprise is having on the savings association.
- Whether the holding company is in compliance with prior commitments to take corrective action.
- Substantial violations of law.

Consulting with State Authorities and the FDIC

Communications with other regulators is essential to ensure a smooth resolution of a problem association. Consultation with state banking supervisors should occur in parallel with examinations, supervisory efforts, and enforcement actions. For example, when considering a supervisory agreement with a state-chartered association, OTS will consult with the state supervisor and solicit concurrence. If OTS issues an Individual Minimum Capital Requirement directive to a state-chartered savings association, OTS will notify the state regulator. 12 CFR §567.3(d)(1) and (3). OTS consults with the FDIC and other appropriate regulatory agencies, as well as state regulators, before taking formal enforcement actions against state-chartered associations.

In coordinating these consultations, be aware of existing information sharing agreements and laws that may govern information sharing between regulators.

TYPES OF ENFORCEMENT ACTIONS

This Section discusses the specific types of enforcement actions, formal and informal, that OTS may take, the regulatory considerations in deciding whether and what type of enforcement action to take, and the procedures for investigating and initiating enforcement actions.

OTS generally attempts to obtain consent to the issuance of an enforcement action from an association's board of directors. Although rare, OTS may not seek consent, for example, in an instance where an immediate cessation to an activity is necessary to halt harm to an association.

Informal Enforcement Actions

When an association's overall condition is sound, but it is necessary to obtain written commitments from an association's board of directors or management to ensure that they will correct the identified problems and weaknesses, OTS may use informal enforcement actions. OTS commonly uses informal actions for problems in the following types of associations:

- Well- or adequately-capitalized associations.
- Associations with a composite rating of 1 or 2.
- Associations with a 3-rating with strong management.

Informal actions put the board and management on notice that OTS has identified problems in case a formal action may be necessary later.

Informal actions are not enforceable in and of themselves. If the association violates or refuses to comply, OTS cannot enforce compliance in federal court or assess civil money penalties for noncompliance but the OTS may take more severe enforcement actions if the institution fails to comply. The effectiveness of the informal tools depends in part on the willingness and ability of the association to correct deficiencies that OTS notes.

OTS has a number of informal enforcement tools available to address unsafe or unsound practices or violations of laws and regulations. Those informal enforcement actions include, but are not limited to, the following actions:

- Meetings with management (see Thrift Activities Regulatory Handbook Section 330).
- Meetings with the board of directors (see Thrift Activities Regulatory Handbook Section 320).
- Board of directors' resolutions. (A document designed to address one or more specific concerns identified by OTS and adopted by the association's board of directors).
- Supervisory letters and directives. (A supervisory letter is a letter signed by the board of directors or management reflecting specific written commitments to take corrective action in response to problems or concerns identified by OTS in its supervision of the association).
- Special examinations.
- Requests for voluntary management changes or reorganizations.
- Notice of deficiency and request for safety and soundness compliance plan.
- Individual Minimum Capital Requirement. (IMCR) Directives. OTS may establish an IMCR for a savings association that varies from the requirement that would otherwise apply to the association. OTS may establish such IMC requirements for a savings association, as it deems necessary on a case-by-case basis, pursuant to 12 CFR § 567.3.

  Minimum capital levels higher than those normally required may be appropriate for savings associations:

  — Needing special supervisory attention.

  — Exhibiting a high degree of exposure to interest rate risk, credit risk, and other risks due to nontraditional activities.

  — Experiencing poor liquidity or cash flow problems due to weak credit quality, operational losses, and other factors.

  Associations have the opportunity to respond in writing to OTS notification of imposition of an IMCR. Failure to satisfy an IMCR may constitute grounds for issuance of a capital directive to the association, or other formal enforcement action.

If informal tools do not resolve the problem, OTS will use formal enforcement tools. An association's unwillingness to comply with an appropriate informal remedy is a significant factor in determining whether a formal enforcement response is appropriate.

Formal Enforcement Actions

A formal enforcement action is both written and enforceable under the FDIA. 12 USC § 1818(b) and § 1831o. Formal actions are appropriate when an association has significant problems, especially

when there is a threat of harm to the association, depositors, or the public. OTS will use formal enforcement actions when informal remedial actions are inadequate, ineffective, or otherwise unlikely to secure correction of safety and soundness or compliance problems.

Because formal actions are enforceable, OTS can assess civil money penalties against associations and individuals for noncompliance with a formal agreement, consent order, or a cease and desist order. OTS can also request a federal court to issue an injunction requiring the association to comply with an order. Unlike informal actions, formal enforcement actions are public.

Formal enforcement actions include the following:

- Formal written agreements pursuant to 12 USC §1818(b). These agreements include Supervisory Agreements and Capital Directives under 12 CFR §567. We discuss Supervisory Agreements in a separate section. A capital directive is an order designed for establishing and enforcing capital levels and for taking capital-related action. OTS may issue a capital directive based on any of the following:
  - — A savings association's noncompliance with a capital requirement established under 12 CFR §§ 567.2 and 567.3.
  - — By a written agreement under 12 USC §1464(s).
  - — As a condition for approval of an application.

OTS rarely uses capital directives because the timing requirements and supervisory restrictions contained in PCA will usually occur prior to a capital directive.

- Cease-and-desist orders (C&Ds). 12 USC §1818(b).
- Temporary C&Ds pursuant to 12 USC §1818(c).
- Removal and/or prohibition orders (R & Ps).
- Temporary suspensions for certain criminal indictments.
- Civil money penalties (CMPs).
- Prompt Corrective Action (PCA) directives, including capital plans under 12 USC §1831o and 12 CFR Part 565 (including temporary restrictions on operations).
- Orders enforcing safety and soundness standards.
- Safety and soundness orders for failure to comply with a notice of deficiency or compliance plan under 12 USC §1831p-1 and 12 CFR Part 570.
- Injunctive actions.
- Immediate suspensions during removal and prohibition proceedings.
- Temporary suspension of insurance.
- Termination of insurance.[3]
- Suspension or debarment of attorneys, accountants, and accounting firms (Part 513).
- Conservatorships and receiverships.
- Enforcement of orders in United States District Court.

We discuss below the formal enforcement actions that OTS most frequently uses.

Supervisory Agreements

Supervisory agreements are formal written agreements, and OTS uses them only with savings associations or their holding companies that are subject to OTS's continuing supervision and jurisdiction, not with individuals or other entities. OTS may use supervisory agreements to require savings associations or holding companies to cease any statutory or regulatory violation or unsafe or unsound practice. The agreements may also require affirmative corrective action to address any existing violations, management or operational deficiencies, or other unsound practices. In short, they may include the same broad range of provisions that OTS may incorporate into C&D orders.

Violations of supervisory agreements, unlike violations of other types of formal enforcement actions, are not enforceable in federal court. 12

[3] The FDIC terminates insurance of accounts; however, OTS may recommend termination of insurance.

USC § 1818 (i). However, a violation of a supervisory agreement may form the basis for the possible assessment of CMPs, C&D actions, and R&P actions. To ensure that supervisory agreements, if violated, will properly form the basis for other enforcement actions, each supervisory agreement should state that "the Agreement is a 'written agreement' for the purposes of Section 8 of the Federal Deposit Insurance Act, 12 USC § 1818."

Cease-and-Desist Orders

A C&D order normally requires a halt to illegal, unsafe, or unsound activities. OTS may issue a C&D order in response to violations of federal banking, securities, or other laws by institutions or individuals, or if it believes that an unsafe and unsound practice or violation is about to occur.

OTS authority for issuing C&D orders is the Federal Deposit Insurance Act (FDIA), 12 USC § 1818(b). OTS will issue a C&D order if one of the following factors is present:

- An unsafe or unsound practice.
- A violation of law, rule, or regulation.
- A violation of any condition imposed in writing in connection with the granting of an application, or any written agreement with OTS or the FDIC.

OTS can issue a C&D order by consent or following a formal administrative hearing.

OTS can issue a C&D order against a savings association, its service corporation or subsidiary, an IAP, a savings and loan holding company, a holding company subsidiary, or service providers.

If an entity or individual fails to comply with a final order, the OTS may seek enforcement of the order through the United States District Court. Violations of an order may form the basis for possible civil money penalties and for removal and prohibition actions. A party subject to the C&D may apply for modification or termination of the order.

Temporary Cease-and-Desist Orders

OTS uses temporary C&D orders to address situations requiring immediate action. To issue a temporary order, OTS first issues a notice of charges, which also initiates a proceeding to obtain a permanent C&D order. In the notice of charges, OTS states that it has determined that there is a violation, an unsafe or unsound practice, or a threatened violation or practice that is likely to result in one or more of the following conditions:

- Insolvency or significant dissipation of assets or earnings.
- Weakening of the association's condition.
- Prejudice to the interests of the depositors before the completion of the C&D proceeding.

A temporary C&D order may require affirmative action to prevent insolvency, dissipation of assets, a weakened condition, or prejudice. For example, OTS may use a temporary C&D order to require that an association restore its books and records to a complete and accurate state under the following conditions:

- An association's books and records are so incomplete or inaccurate that OTS is unable, through the normal supervisory process, to determine the financial condition of the association.
- An association's books and records are so incomplete or inaccurate that OTS cannot determine the details or purpose of a transaction that may have a material effect on the association's financial condition.

OTS may also use a temporary C&D to order cessation of any activity pending the completion of the C&D proceeding. For example, OTS may issue a temporary C&D to freeze assets pending the outcome of litigation or to require immediate change in management. OTS can also require cessation of activities causing incomplete or inaccurate books or records.

A temporary C&D order terminates automatically when OTS dismisses the charges in the notice initiating the C&D proceeding or when a permanent C&D against the same party becomes effective.

Orders of Removal and Prohibition

OTS can remove an IAP from office and prohibit a person or entity from further participation in an association's affairs under Section 8(e) of the FDIA, 12 USC § 1818(e), if all of the following circumstances occur:

- The IAP directly or indirectly engaged in any of the following practices:
  - — Violated a law, regulation, or final C&D.
  - — Violated any condition imposed in writing by the appropriate federal banking agency in connection with the grant of any application or other request by the depository institution.
  - — Violated any written agreement between the depository institution and the agency.
  - — Engaged or participated in any unsafe or unsound practice with respect to any insured depository institution or business institution.
  - — Committed or engaged in any act, omission, or practice that constitutes a breach of fiduciary duty.
- As a result of the violation, unsafe or unsound practice, or breach of fiduciary duty described above, any of the following occurred:
  - — The insured depository institution suffered or will probably suffer financial loss or other damage.
  - — The interests of the insured depository institution's depositors have been or could be prejudiced.
  - — The IAP received financial gain or other benefit from the violation, practice, or breach.
- The violation, unsafe or unsound practice, or breach of fiduciary duty:
  - — Involves personal dishonesty.
  - — Demonstrates a willful or continuing disregard for the safety or soundness of the insured depository institution or business institution.

An R&P order has industry wide effect and permanently bars an individual from holding office in, being employed by, or participating in any manner in the conduct of the affairs of any insured depository institution, including credit unions, and from working for any depository institution regulatory agency. Individuals who violate R&P orders are subject to criminal penalties. Removed or prohibited individuals may apply for modification or termination of the R&P order. Anyone convicted of a criminal offense involving dishonesty or breach of trust, or who has agreed to enter into a pre-trial diversion or similar program in connection with such a prosecution, is automatically subject to an industry-wide prohibition by operation of law. 12 USC § 1829.

Temporary Suspensions

OTS may issue an order temporarily suspending an individual from a position in conjunction with a notice of intention to remove or prohibit the individual. 12 USC § 1818(e)(3). By statute, OTS can issue a temporary suspension only if the suspension is necessary to protect the interests of the depository institution or its depositors. The suspension remains in effect pending the removal or prohibition proceeding initiated by the notice, unless a district court stays the suspension as provided by the FDIA. 12 USC §1818(f).

OTS staff must adequately document violations or unsound practices underlying the temporary suspension. OTS will use the documentation when presenting its action to a reviewing court. Appropriate documentation may include the following materials:

- Examination reports.
- Sworn testimony.
- Other materials documenting violations or personal gain to the individual.
- Periodic reports to OTS showing a decline in an association's financial condition.

A suspended individual may apply to the U.S. District Court for an injunction or stay of the temporary suspension, within 10 days of service of the suspension. The court will consider both the reasonableness of OTS's decision to issue the sus-

pension and the traditional standards for injunctive relief.

OTS has authority to temporarily suspend or remove an individual charged with committing or participating in a crime involving dishonesty or breach of trust, which is punishable by a term of imprisonment exceeding one year, if the individual's continued service poses a threat to the interests of the association's depositors or threatens to impair public confidence in the association. 12 USC §1818(g). In such cases, the temporarily suspended or prohibited individual may request an opportunity to appear before the agency to show that his or her continued participation does not pose a threat to the interests of depositors or threaten to impair public confidence. The suspension or prohibition remains in effect until resolution of the criminal charges or termination of the order of suspension.

Civil Money Penalties

OTS possesses statutory authority under the FDIA and other statutes to assess CMPs against savings associations, their service corporations or subsidiaries, savings and loan holding companies, and IAPs. Assessment of a CMP is appropriate for any of the following violations:

- Violations of any laws or regulation.
- Violations of the terms of any final order or temporary order.
- Violations of any condition OTS imposed in writing in connection with the granting of any application or other request by the association.
- Violations of any written agreement between the association and OTS.
- Breaches of fiduciary duty.
- Failure to maintain adequate records.
- Failure to file, or filing late or inaccurate OTS-required reports.
- Unsafe or unsound practices.

When assessing a CMP, OTS should consider the following factors:

- Financial resources and good faith of the person, association, or company.
- Whether the person, association, or company will make financial resources available.
- The gravity of the violation.
- The history of previous violations.
- Any such other matters as justice may require.

OTS uses the Civil Money Penalty Form in Regulatory Bulletin (RB) 18-3a as guidance in considering and assessing CMPs. The form consists of the Civil Money Penalty Tier Matrix to determine the tier of a violation, and the Civil Money Penalty Calculation Sheet to assess a penalty amount for the violation. There are two tier matrices: the General Tier Matrix and the Reporting Violation Tier Matrix.

While OTS expects to use these matrices in all cases where it is considering an assessment, they are not substitutes for sound supervisory judgment. Individual cases may possess particularly egregious or mitigating characteristics not included as factors in the matrices.

For detailed information on the application of civil money penalties, refer to the FFIEC Policy Statement on Civil Money Penalties (6/3/98) and to RB 18-3a, Enforcement Policy Statement on Civil Money Penalties (7/30/93).

Prompt Corrective Action

Prompt Corrective Action (PCA) is triggered by an association's capital category, as defined in 12 USC §1831o and 12 CFR Part 565. Depending on an association's PCA capital category, certain restrictions and actions are automatically imposed by operation of law. Other PCA actions are discretionary. (See Appendix).

Capital Plans

In addition to mandatory and discretionary operating restrictions, the FDIA requires all savings associations with a rating below adequately capitalized to submit a timely capital restoration plan (Capital Plan) within 45 days of receiving notice or being deemed to have notice of becoming undercapitalized. OTS regulations provide the

timing, content, and approval standards for Capital Plans in 12 CFR § 565.5. The Capital Plan must explain in detail the proposed strategy for becoming, at a minimum, adequately capitalized, and for accomplishing the association's overall objectives.

Under 12 USC § 1831o(e)(2), OTS must consider various factors in determining whether to approve the plan. These factors include, but are not limited to, the following criteria:

- How the association will comply with restrictions and requirements under the FDIA.
- The association's proposal to become adequately capitalized.
- The association's activities.
- Whether the association's assumptions are realistic.
- Likelihood of success.
- Risk exposure.

Each controlling company of an undercapitalized association must guarantee that the association will comply with the Capital Plan until adequately capitalized (on average) during four consecutive quarters, and provide adequate assurances of performance. 12 USC § 1831o(e)(2)(c)(ii).

If OTS approves the Capital Plan submitted by the association, it becomes the basis for a PCA Directive along with any mandatory or discretionary operating restrictions applicable to the association. If OTS determines that the association's Capital Plan is not acceptable or if the association fails to file one, OTS issues a PCA Directive. The PCA Directive becomes the basis for curtailing certain activities, and mandating the steps necessary to either increase capital to acceptable levels, or otherwise move the association toward resolution. See discussion in the Appendix A on Capital Plans.

Prompt Corrective Action (PCA) Directives

The FDIA requires that the agencies take prompt enforcement against undercapitalized institutions. Under PCA standards, an institution is in one of five capital categories: well capitalized; adequately capitalized; undercapitalized; significantly undercapitalized; and critically undercapitalized.

Mandatory, discretionary, and presumed restrictions and sanctions apply for institutions in the three undercapitalized categories. You will find additional information regarding the five capital categories in the Thrift Activities Regulatory Handbook Section 120, Capital Adequacy. A PCA directive establishes a capital-based supervisory scheme that requires OTS to place increasingly stringent restrictions on associations as regulatory capital levels decline. The primary objective of PCA is "to resolve problems of insured depository institutions at the least possible long-term loss to the deposit insurance fund." 12 USC § 1831 o(a)(1).

PCA mandates the imposition of certain restrictions once an association falls below the well-capitalized category. Most of the restrictions are limited to associations at the undercapitalized level or below. The following two restrictions, however, pertain to all adequately capitalized associations:

- No association can make a capital distribution if it results in undercapitalization; and
- The FDIC restricts associations from receiving brokered deposits unless they meet the well-capitalized definition.

For associations at the undercapitalized level and below, there are additional mandatory operating restrictions that apply automatically without regard to whether a PCA directive is in place. These restrictions, set out in 12 USC § 1831o(e) and 12 CFR § 565.6(a)(2), include the following actions:

- Restricting asset growth.
- Restricting capital distributions and certain management fees.
- Limiting the ability to make acquisitions, branch, or enter new lines of business.
- Requiring compliance with a capital restoration plan submitted by the association.
- Monitoring by OTS. (This may include more frequent field visits by OTS or written quarterly reports from the board of directors on adherence to the PCA restrictions).

In addition to the mandatory restrictions, the PCA regulations provide OTS with authority to apply a

wide range of discretionary remedies. 12 USC § 1831o(e)(5) and §1831o(f)(5). OTS should impose the following discretionary restrictions when conditions warrant:

- Require recapitalization.
- Restrict transactions with affiliates.
- Restrict interest rates paid.
- Restrict asset growth more stringently than required by statute.
- Restrict activities (for example, banning certain types of lending).
- Improve management (for example, mandating the election of a new board of directors, dismissing current directors and members of senior management, or requiring the hiring of certain qualified employees subject to OTS approval). 12 USC § 1831o(f)(2)(F) and 12 CFR §§ 565.6 and 565.9.
- Prohibit deposits from correspondent banks.
- Require prior approval for capital distributions by a bank holding company.
- Require divestiture.
- Restrict executive or senior officer compensation more stringently than required by statute (for example, restricting bonuses).12 USC § 1831o(f)(4).
- Take any other action necessary to resolve the problems of the association at the least possible long term loss to the insurance fund.

The above provisions apply to associations that fail to submit and implement capital plans. OTS regulations at 12 CFR § 565.7 pertain to the process for issuance of PCA directives. See also Appendix A under PCA Directives.

In addition to the PCA remedies available for undercapitalized savings associations, the statutory framework allows the OTS to reclassify an association's PCA category if it operates in an unsafe and unsound condition. 12 U.S.C § 1831o(g) and 12 CFR § 565.8. Associations may request a hearing regarding the reclassification and the restrictions under 12 CFR § 565.8(a)(5) and (6). Once the OTS has implemented a reclassification, an association can petition the OTS for a PCA category upgrade if it successfully rectifies the unsafe and unsound conditions. See Appendix A under PCA Reclassifications.

Orders Enforcing Safety and Soundness Standards

OTS also has authority to issue a Safety and Soundness Order against a savings association under 12 USC § 1831p-1 and the implementing regulations, 12 CFR Part 570. The process begins with OTS issuing a notification to the association of its failure to meet the safety and soundness standards, and requesting that the association submit a compliance plan.

Generally, this tool addresses unsafe and unsound conduct that is not reflected in capital levels. These notices of deficiencies may also address specific problems in well- or adequately-capitalized associations. OTS generally only uses Part 570 safety and soundness notices of deficiency when the following conditions are present:

- The problems or weaknesses are narrow in scope and correctable.
- OTS is confident of the board's and management's commitment and ability to correct problems or weaknesses.

If the association fails to submit a compliance plan, or fails to comply with an approved compliance plan, OTS may issue a Safety and Soundness Order. The association has the right to respond in writing to the proposed issuance of an order. There are serious consequences for an association's failure to comply with a Safety and Soundness Order. OTS can impose CMPs or seek enforcement through judicial or administrative proceedings.

POST-ENFORCEMENT ACTIONS

Checking for Compliance with Outstanding Agreements and Orders

The recurrence of a problem previously addressed by an informal method of supervision, such as a supervisory directive, raises a presumption that OTS will pursue a C&D action or assess a CMP. That is, a material violation of an informal enforcement action should cause OTS to consider a

C&D action or a CMP assessment, unless there are substantial mitigating factors.

A significant violation of a formal enforcement order raises a presumption that OTS will take a more severe formal enforcement action (for instance, CMPs against the board or management if the association has failed to comply with a C&D order).

During every examination, regardless of the type of examination, examiners will expressly check for compliance with each outstanding directive, agreement, or order. Examiners must document compliance or noncompliance in the Report of Examination (ROE). The terms of the directive, agreement, or order will dictate the scope of the inquiry. For example, an agreement requiring an association to develop and adopt effective, written lending procedures necessitates that examiners review the procedures for clarity, effectiveness, and proof that the board of directors adopted them. An agreement that the association must comply fully with new loan procedures requires a review of a sample of loans for compliance with those procedures. This review should be in addition to the normal loan review for compliance with applicable regulations and safety and soundness standards. (See Thrift Activities Regulatory Handbook Section 060, Examination Strategy, Scoping, and Management).

Documentation

Throughout this Handbook Section we mention the importance of thorough documentation that is required for taking supervisory and enforcement action. In the event an association violates a final order that OTS may have to enforce by bringing court action, OTS will rely on examiners' determination of the source of noncompliance (or other conduct), which may be due to the association's administrative oversight, lack of knowledge or skill, or willful disregard. Discussions with management should be summarized in a written report. This report should also include management's oral explanations of why such violations occurred and OTS's opinion as to the necessity of further enforcement action.

In all cases, OTS should obtain clear documentary evidence of the violations or conduct to provide evidence if OTS issues an order or must enforce the order in District Court.

Termination or Modification of Enforcement Actions

Generally, OTS does not terminate an enforcement action until the association has complied with all the articles in the enforcement action document.

OTS must explain, in writing, a decision to terminate or modify an enforcement action. An OTS examination documenting compliance with the enforcement action is usually a prerequisite to removal of the action unless OTS can obtain the appropriate documentation to support such modification or termination without an OTS examination. In limited instances, OTS will permit a modification or termination of an enforcement action without an OTS examination if deemed appropriate.

METHODS OF GATHERING INFORMATION

Regular and Special Examinations

Generally, OTS will undertake informal means of obtaining information before requesting a formal examination with subpoena power. OTS will seek out and use reliable information from savings associations and their affiliates, employees, and agents.

Because of OTS's authority to examine the records of any savings association and that association's affiliates, OTS does not need to issue subpoenas to compel the production of the records of the savings association or their affiliates. HOLA § 5(d)(1)(B) entitles OTS to prompt and complete access to all association personnel and agents, and to all association documents. Examiners should notify Regional Counsel immediately if the association or its personnel refuse to supply association records or otherwise obstructs the progress of an OTS examination. Section 5(d)(1)(B) grants OTS specific authority to go to federal court to obtain an order requiring that the association provide such access.

Informal requests to interview persons outside of the association or to review records of a borrower

or other entity that is not a savings association or its affiliate may also be informative.

The Gramm-Leach-Bliley Act [Pub. L. No. 106-102, 113 Stat. 1338 (1999)] established a framework of procedural requirements and criteria for working with functionally-related entities, which may be a subsidiary, sister corporation, or other depository institution engaged in activities regulated by another regulatory agency, such as the SEC. OTS will work cooperatively with the primary regulator of the entity to request information and reports. In limited circumstances, if the regulator is unable or unwilling to obtain the information, OTS can request the information directly from the entity. If the information is insufficient, OTS can, in some instances, conduct an on-site examination of the entity if OTS can meet certain requirements showing OTS's need for the information.

OTS may also obtain information from publicly available sources of information, such as land record offices or state corporation commissions.

REFERENCES

United States Code (12 USC)

§ 1464(d)	Regulatory Authority
§ 1464(s)(2)	Individual Minimum Capital Requirement
§ 1464(s)(4)	Directive to Increase Capital
§ 1467a	Regulation of Holding Companies
§ 1467a(g)	Administration and Enforcement
§ 1813(u)	Institution-Affiliated Party
§ 1817(j)	Change in Control of Insured Depository Institutions
§ 1818(b)	Cease-and-Desist Proceedings
§ 1818(e)	Removal and Prohibition Authority
§ 1818(f)	Stay of Suspension and/or Prohibition of Institution-Affiliated Party
§ 1818(g)	Suspension or Removal of Institution-Affiliated Party Charged with Felony
§ 1818(i)(1)	Proceedings to Enforce Compliance
§ 1818(i)(2)	Civil Money Penalties
§ 1818(i)(4)	Prejudgment Attachment
§ 1818(n)	Subpoena Power
§ 1820(c)	Subpoena Power
§ 1831o	Prompt Corrective Action
§ 1831p-1	Actions to be Taken for Failure to Comply with Safety and Soundness Standards

Code of Federal Regulations (12 CFR)

Part 508	Removals, Suspensions, and Prohibitions Where a Crime Is Charged or Proven
§ 509 et seq	Adjudicatory Proceedings
§ 512 et seq	Investigative and Formal Examination Proceedings
Part 513	Practice Before the Office
Part 565	Prompt Corrective Action
§ 565.7	Directives to Take Prompt Corrective Action
§ 567.3	Individual Minimum Capital Requirements
§ 567.4	Capital Directives
Part 570	Safety and Soundness Orders

Office of Thrift Supervision Bulletins

RB 18	Issuance of Enforcement Policies
RB 18-1c	General Enforcement Policy
RB 18-3a	Enforcement Policy Statement on Civil Money Penalties

Other References

FFIEC Interagency Policy Regarding the Assessment of Civil Money Penalties by the Federal Financial Institutions Regulatory Agencies.

Enforcement Actions Program

Examination Objectives

To determine if the institution and individuals are in compliance with the requirements of outstanding agreements or orders.

To determine if new or additional enforcement actions need to be taken to correct deficiencies.

Examination Procedures

Level I

Wkp. Ref.

1. Review any written enforcement action that is in effect between the institution and the OTS, FDIC, or state supervisory authorities, if applicable.

2. Identify what the institution or individual is required to do or is prohibited from doing by the enforcement action.

3. Evaluate any self-policing system established. That is, assess how the system has been communicated to the officers and employees and determine whether the appropriate employees are aware of any corrective action needed.

4. Review the appropriate areas of concern to determine whether or not the institution or individual is in compliance with the provisions of the enforcement action. Work papers should fully support all conclusions.

5. If compliance is determined, summarize the findings, including comments for the report of examination (ROE) as necessary.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

6. If noncompliance is found, proceed to Level II procedures.

7. Discuss overall examination findings with the EIC.

   - If a composite rating of 3, 4, or 5 is anticipated, determine what enforcement action(s), if any, is(are) necessary.
   - If a composite rating of 3 is anticipated, determine if there are any mitigating factors to warrant only informal enforcement action(s).
   - Document your decision and proceed to Level II procedures.

Level II

8. Determine if there is another regulatory agency that is the primary regulator of the entity from whom you must obtain information. If so, work with your region's functional regulation contact to coordinate your information requests and any examination of a functionally-regulated entity.

9. If documents required by the enforcement action (e.g., appraisal, financial statements) cannot be located, request them in writing from management. If you fail to receive the requested material, request a written response. If management will only respond orally, assure that two examiners are present and immediately write a summary of the response signed by both examiners.

10. Gather documents or materials that support the noncompliance (poor appraisals, modified notes, loan register, loans in process ledger, etc.). Separate and identify all appropriate work papers, ensuring they are factual, complete, and do not contain expressions of examiner opinion.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Wkp. Ref.

11. Assess whether noncompliance is due to the association's administrative oversight, lack of knowledge, or willful disregard. State facts, be objective, and avoid speculation.

12. Formulate recommendations for any necessary supervisory action; e.g., if a previous supervisory agreement is violated, a C&D or assessment of a civil money penalty may be appropriate.

13. The EIC must notify the regional office's legal staff by telephone and report the findings, recommending any further enforcement action.

14. Per discussion with EIC or regional office staff, write an interim report detailing your findings.

15. Prepare all comments and conclusions for the ROE as necessary.

Examiner's Summary, Recommendations, and Comments

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Prompt Corrective Action Guidelines

This document updates and incorporates all previous guidance issued by OTS on Prompt Corrective Action (PCA) into one single policy issuance. This document supersedes all previously issued guidance. The PCA statutory, regulatory, and policy framework provides OTS with effective supervisory remedies to minimize losses to the deposit insurance fund. [1]

The statutory authority for PCA is found in the Federal Deposit Insurance Act (FDIA) at 12 USC 1831o. OTS has implemented that authority in regulations at 12 CFR Part 565. PCA requires that certain operating restrictions take effect when an institution is undercapitalized. The statute creates five capital categories, which are defined as follows by OTS at 12 CFR §565.4(b) (consistent with the other banking agencies):

PCA Categories

Thrifts fall into one of five PCA categories. The PCA minimum requirements are as follows:

	Total Risk-Based		Tier 1/Risk-Based		Tier 1/Leverage
Well Capitalized*	10% or greater	*and*	6% or greater	*and*	5% or greater
Adequately Capitalized	8% or greater	*and*	4% or greater	*and*	4% or greater (3% for 1-rated)
Undercapitalized	Less than 8%	*or*	Less than 4%	*or*	Less than 4% (except for 1-rated)
Significantly Undercapitalized	Less than 6%	*or*	Less than 3%	*or*	Less than 3%
Critically Undercapitalized	Has a ratio of tangible equity to total assets that is equal to or less than 2%. Tangible equity is defined in 12 CFR § 565.2(f) and differs from the definition of tangible capital under FIRREA.				

[1] OTS has additional powers under the Home Owners Loan Act (HOLA) for a thrift's failure to meet capital requirements as detailed in 12 CFR 567.10. This document does not discuss the HOLA capital provisions which are addressed in Thrift Activities Handbook Section 120 Capital Adequacy.

* To be well capitalized, a thrift also cannot be subject to a higher capital requirement imposed by OTS.

Notice of Capital Category and Mandatory and Discretionary Operating Restrictions

OTS deems that thrifts have received notice of their capital category as of the date they file a Thrift Financial Report (TFR) or when OTS transmits a final report of examination (ROE). A thrift must also notify OTS of any event that results in the lowering of a PCA capital category within 15 days of the material event that caused the decreased capital. 12 CFR §565.3(c)(2). In addition, OTS should provide written notice of a thrift's reclassified PCA status after receipt of a TFR, with the transmittal of a ROE, or upon learning of an event that results in a reclassification in capital category. The notice from OTS should include the mandatory and any discretionary operating restrictions (discussed below) applicable to thrifts in the designated category (see Chart 1 - PCA Categories). The restrictions are effective immediately upon the earlier of being deemed to have notice or receiving written notice of a capital category reclassification.

PCA requires OTS to apply progressively more significant restrictions on an institution's operations as its capital category falls. PCA mandates the imposition of two restrictions once a thrift falls below the well capitalized category. First, no thrift can make a capital distribution or pay certain management fees if it results in its becoming undercapitalized. Second, the FDIC restricts thrifts from receiving brokered deposits unless they meet the well capitalized definition. The remaining mandatory operating restrictions apply to institutions in the undercapitalized (or below) category.

For thrifts at the undercapitalized level and below, the additional mandatory operating restrictions include the following, found at 12 CFR § 565.6:

- Restricting capital distributions and certain management fees.
- Restricting asset growth.
- Limiting the ability to make acquisitions, branch, or enter new lines of business without prior agency approval.
- Compliance with a capital restoration plan submitted by the association.
- Requiring that OTS monitor the condition of the thrift.

All mandatory restrictions are effective immediately upon receiving or being deemed to have received notice of being less than well capitalized.

In addition to the mandatory restrictions, the PCA regulations provide OTS with authority to apply a wide range of discretionary remedies. Some of these provisions allow for directing changes in management should a thrift fall into the significantly undercapitalized level. OTS can mandate the election of a new board of directors, dismiss current directors and members of senior management, and require the hiring of certain qualified employees (subject to OTS approval) deemed necessary for safe and sound operations. 12 USC 1831o(f)(2)(F); 12 CFR §§ 565.6 and 565.9. Other discretionary remedies include restrictions or bans on certain types of lending, limits on bonuses, prior approval of certain contracts, and other restrictions that OTS deems appropriate.

If a thrift remains critically undercapitalized for ninety days, OTS must appoint a receiver or a conservator, or take such other action approved by the FDIC. (Capital failure as defined under the PCA statute is just one of the grounds for placing a thrift under a conservator or receiver.)

Even when thrifts are well capitalized or adequately capitalized under the PCA statute and regulations, OTS may exercise other authority to restrict a thrift's operations when capital levels are not commensurate with its balance sheet risk. OTS may use Individual Minimum Capital Requirements, Part 570 Compliance Plans, Supervisory Agreements, and/or Cease and Desist Orders .

Capital Restoration Plan

In addition to the mandatory and discretionary operating restrictions, the FDIA requires all thrifts below adequately capitalized to submit a capital restoration plan (Capital Plan) within forty-five days of their receiving notice or being deemed to

have notice of becoming undercapitalized. This section discusses the contents and approval of a Capital Plan in detail.

OTS regulations explain the timing, content, and approval standards for Capital Plans at 12 CFR § 565.5. The agency may alter the timing with proper cause.

Pursuant to agency policy, the Capital Plan must explain in detail the proposed strategy for becoming, at a minimum, adequately capitalized and for accomplishing the thrift's overall objectives. The plan should include:

- A detailed discussion of the following information:
  - — The steps the association will take to become adequately capitalized, including underlying assumptions and proposed strategies.
  - — Methodologies for forecasting the disposition of problem assets and the levels of expected charge-offs.
  - — Any substantial changes in assets and liabilities.
  - — The types and levels of activities in which the thrift plans to engage.
  - — Strategies to control operating expenses, interest-rate risk, credit risk, and other significant risk exposures.
- Quarterly financial projections that generally follow the TFR, extending four quarters beyond the date the association becomes adequately capitalized. The projections should show the following information:
  - — Progressively higher capital levels for complying with adequately capitalized standards.
  - — Levels of core and net earnings.
  - — Any capital infusions (specific steps must be taken within 6 months of becoming undercapitalized).
  - — Compliance with applicable statutory or regulatory restrictions and OTS policies.

  The thrift must base its projections on the following realistic assumptions and rates:
  - — Current Treasury rates and the implied interest rate forecast embedded in the existing yield curve for Treasury securities, with spreads over Treasuries on incremental assets and liabilities consistent with prevailing market spreads.
  - — Prepayment rates that reflect the market's consensus estimate for similar mortgage loans.
  - — Loan origination rates using recent experience and taking into consideration current national and regional economic conditions.
  - — The institution may use OTS's quarterly updates on interest rates. The thrift can request a copy from the OTS Regional Office shortly after each quarter-end.
- A standard form of guarantee and assurance from all controlling companies, as required under 12 USC 1831o. In a tiered holding company structure, each controlling company must provide a standard form of guarantee and assurance signed by a majority of the board of directors or a duly authorized official. The guarantee does not supersede any existing capital maintenance agreements. A copy of the standard form can be obtained from the Chief Counsel's Office.
- A commitment in the Capital Plan to provide the Regional Director with quarterly variance reports comparing actual results to projected targets established in the capital plan within 30 days (or sooner if the institution drops another PCA Capital category) following the close of each calendar quarter. OTS will condition approval of the plan upon submission of these variance reports. Failure to file required variance reports may result in enforcement action including civil money penalties. Material variances are grounds for terminating a capital plan approval.

After receipt of the Capital Plan, OTS has sixty days to review the contents and decide whether to approve or deny. If the institution is critically undercapitalized, the FDIC will conduct a joint review of the proposed capital plan. By statute, 12 USC 1831o(e)(2), each agency must consider the following factors in determining whether to approve the plan:

- Does the Capital Plan specify the following information:
  - — The steps proposed by the institution to become adequately capitalized, and the anticipated capital levels for each quarter contained in the plan.
  - — How the institution will comply with the restrictions and requirements under the FDIA.
  - — The types and levels of activities that the institution proposes to engage in, and such other information OTS may require.
- Has the institution based its capital plan on realistic assumptions and is it likely to succeed in restoring the institution's capital?
- Does the Capital Plan demonstrate that the plan will not appreciably increase the institution's exposure to risk (including credit, interest-rate, and other types of risk)?
- Does each controlling company of the undercapitalized institution:
  - — Guarantee that the institution will comply with the plan until adequately capitalized (on average) during four consecutive quarters?
  - — Provide appropriate assurances of performance?

PCA Directive

Whether or not OTS approves the Capital Plan, OTS regulations mandate issuing a directive to take prompt corrective action. 12 CFR §565.7 (PCA Directive).

If the Regional Director approves the Capital Plan submitted by the thrift then it becomes the basis for the PCA Directive along with any mandatory or discretionary operating restrictions applicable to the thrift (as discussed above). If the Regional Director determines that the thrift's Capital Plan is not acceptable or it fails to file one, the PCA Directive becomes the basis for imposing the mandatory and discretionary restrictions and directing the steps necessary to either increase capital to acceptable levels or otherwise move the thrift toward resolution.

The sequence for issuing the PCA Directive is as follows:

- Within fifteen days of reviewing and either approving or denying the thrift's Capital Plan, OTS will issue a "Notice of Intent to Issue a PCA Directive" providing the association with a copy of the proposed PCA Directive and allowing the association 14 calendar days to respond. OTS may shorten the 14-day period if the thrift's financial condition, or other circumstances, warrants.
- The notice of intent should state either that OTS is proposing to issue the directive in conjunction with approval of the Capital Plan, or that the institution has not submitted an acceptable Capital Plan under the standards of PCA. It should also state that OTS has issued the Directive to carry out the purpose of PCA to resolve the institution's problems at the least possible long-term loss to the deposit insurance fund.
- After reviewing the institution's response to the proposed PCA Directive, OTS should make any appropriate revisions.
- Within the fifteen days of issuing the Notice of Intent, OTS should provide the institution with the "Stipulation and Consent to the Issuance of a PCA Directive" for signature by the institution's board of directors.
- Upon receipt of an executed "Stipulation and Consent," OTS should then issue a final PCA Directive that requires compliance with the mandatory PCA sanctions and any discretionary PCA restrictions deemed appropriate.

OTS may issue an immediately effective PCA Directive even if the institution declines to execute the "Stipulation and Consent." OTS can make the Directive effective upon issuance, or within a specified amount of time thereafter.

- In unusual circumstances, where immediate effectiveness of the PCA Directive is crucial, OTS may issue a PCA Directive without prior notice. To do so, OTS must document that immediate effectiveness is necessary to achieve the purpose of PCA. When we issue an immediately effective PCA Directive, the institution has 14 calendar days to submit a written appeal and OTS has 60 days to decide whether or not to modify the PCA Directive. The OTS's PCA regulation permits shortening of the 14-day response period if the financial condition of the institution or other relevant circumstances warrants. The shortened period should allow sufficient time to make a meaningful response. 12 CFR § 565.7. OTS should document in the official file when it shortens the response period.

PCA Reclassifications

In certain situations, the statute allows OTS to reclassify an institution's PCA category to a lower level.

OTS may reclassify a well-capitalized, adequately capitalized or undercapitalized institution to the next lower capital category and subject it to the restrictions applicable to that capital category if the OTS determines that the savings association is in an unsafe or unsound condition or engaged in an unsafe and unsound practice. 12 USC 1831o(g); 12 CFR § 565.8. Once OTS determines that a capital category reclassification is appropriate, all of the mandatory and any appropriate discretionary restrictions for that capital category apply to the institution.

Before reclassifying an institution's PCA capital category, OTS must specify its grounds for doing so and serve the institution with a Notice of Intent to Reclassify. The Notice should include the following items:

- A statement of the institution's capital measures and capital levels and the proposed reclassified category;
- The reasons for reclassification of the institution; and
- The date that the institution may file a written appeal of the proposed reclassification and a request for a hearing, which shall be at least 14 calendar days from the date of service of the notice unless OTS determines that a shorter period is appropriate in light of the financial condition of the savings association or other relevant circumstances.

An institution's failure to file a written response with OTS within the prescribed timeframe shall constitute the institution's consent to the reclassification. In the written response, an institution may request an informal hearing to present oral testimony or witnesses rebutting the reclassification. 12 CFR § 565.8(a)(5)(6). An institution that has been reclassified can petition OTS for a PCA category upgrade once it has successfully rectified the unsafe and unsound conditions.

INTRODUCTION

A thrift's affiliate relationships and transactions can significantly affect the operations and overall financial condition of a savings association. Your review of a thrift's and its subsidiaries' transactions with its affiliates is a critical component of the thrift and holding company examinations. However, the affiliate transaction rules are complex and, at times, confusing. This section will give you a basic understanding of the rules related to affiliate transactions. You should carefully review these transactions to identify any potential risks they pose to the savings association and ultimately to the deposit insurance fund.

During recent years, as competition among providers of financial services increased, companies 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 thrift/affiliate arrangements. OTS's transactions with affiliate rules (§§563.41 and 563.42) (TWA Rules) generally mirror those applicable to banks and serve to limit the risks affiliates present to thrifts.

In many cases, it is appropriate and beneficial for a thrift to engage in business transactions with its affiliates and insiders. OTS, however, may prohibit transactions by regulation or, when contrary to the thrift'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 thrift'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.

Beyond the TWA Rules, additional regulatory standards set forth in §563.43 limit how much and on what terms a thrift may lend to its own insiders (directors, executive officers, principal shareholders and related interests) and insiders of an affiliate.

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 or its subsidiary engages in a transaction with its holding company, any subsidiary of the holding company, or any other entity or person considered an affiliate. You may find evidence of such transactions at any thrift, but the volume of affiliate transactions is usually greater in a holding company structure since intercompany transactions are often an integral part of a company's operations. Due to the potential risk from these transactions, thrifts are subject to the following regulatory standards:

- Individual and aggregate percentage of capital ceilings on the dollar amount of affiliate transactions.
- Arms-length dealings requirement.
- Prohibition of acquisitions of low-quality assets from affiliates.

Table 1

Transactions with Affiliates Guidelines

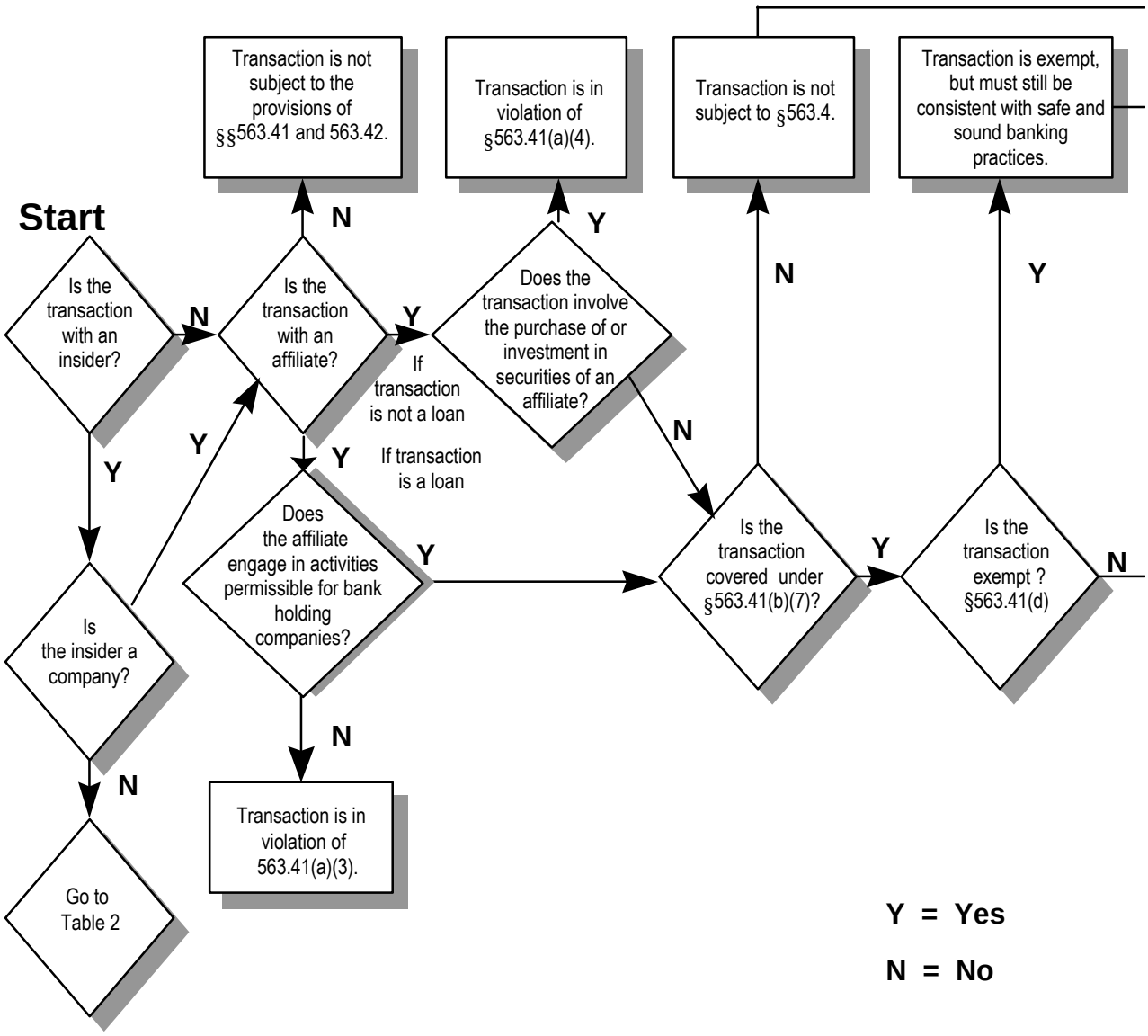
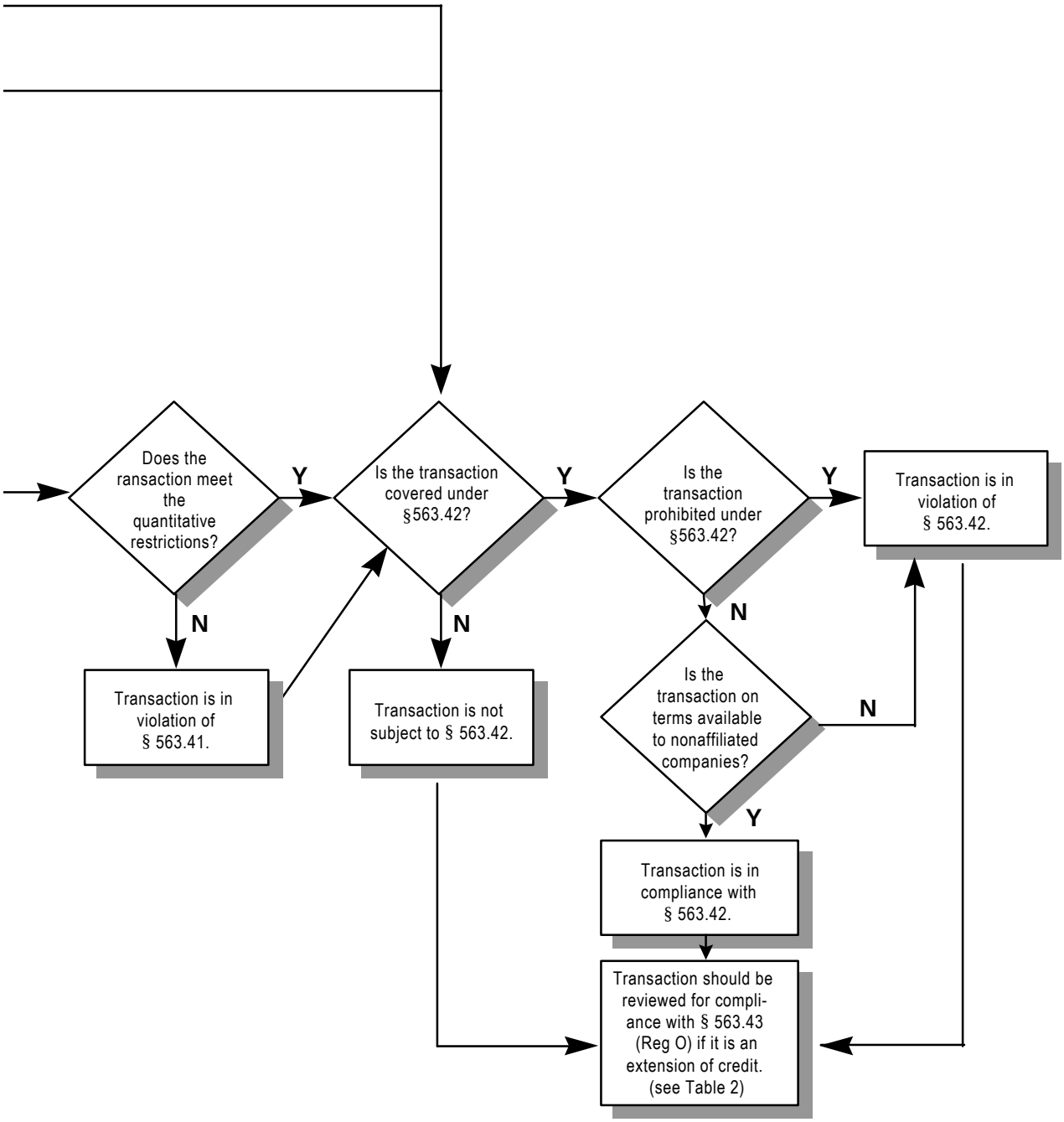


Table 1

Transactions with Affiliates Guidelines



- Collateralization requirements for affiliate credit transactions.
- Prohibition of certain activities.
- Transaction exemption provision.

To help you understand affiliate transactions, the flow chart in Table 1, Transactions with Affiliates Guidelines, presents the following information in a step-by-step manner. Also, you can use Appendix A, Transactions with Affiliates Checklist, to review specific affiliate transactions. The checklist incorporates applicable regulatory standards.

Compliance with 12 CFR §563.41

You should consider all of the following elements to determine whether a transaction is subject to §563.41:

- Is the transaction with an affiliate?
- Does the transaction qualify as a covered transaction?
- Is the transaction an exempt transaction?
- 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, identity the thrift's affiliates. The definition of an "affiliate" includes the following entities:

- A company that controls the savings association and any other company it controls.
- A bank or savings association subsidiary of the savings association.
- A 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.
- A company in which a majority of directors, partners, or trustees constitute a majority of the persons holding office with the savings association or any company that controls the savings association.
- A company, including a real estate investment trust, that the savings association or any subsidiary or affiliate of the thrift, sponsors and advises on a contractual basis, or an investment company for which a savings association or any affiliate thereof is an investment advisor as defined in Section 2(a)(20) of the Investment Company Act of 1940, 15 U.S.C. 80a-2(a)(2).
- A company that OTS or the Board of Governors of the Federal Reserve System determines by regulation or order to have a relationship with the savings association or any subsidiary or affiliate such that covered transactions by the savings association or its subsidiary with that company may be affected by the relationship to the detriment of the savings association or its subsidiary.
- A company that OTS determines presents a risk to the safety or soundness of the savings association, based on the nature of the activities conducted by the company, amount of transactions with the savings association or its subsidiaries, financial condition of the company or its parent association, or other supervisory factors.

Additionally, the thrift should treat any transaction that it or its subsidiary has with any person as a transaction with an affiliate if the proceeds of the transaction are used for the benefit of, or transferred to, an affiliate.

A company or shareholder has *control* over another company if the company or shareholder meets one of the following criteria:

- Directly or indirectly, or by acting in concert with one or more persons, controls, or has the power to vote, 25 percent or more of any class of voting securities.
- Directly or indirectly, or by acting in concert, controls the company under 12 CFR §574.4(a), or is presumed to control the company under §574.4(b), and the control has not been rebutted.

Additionally, for purposes of the TWA Rules, a subsidiary of a savings association is any company the savings association controls according to Part 574.

In general, OTS does not consider subsidiaries of the savings association as affiliates of the savings association. There are, however, some exceptions to this rule. The following subsidiaries are considered affiliates:

- Bank and thrift subsidiaries of a savings association.
- Any company that is a subsidiary and an affiliate (for example, when a holding company and its thrift own controlling shares of the company).
- Any subsidiary that OTS or the Federal Reserve Board (FRB) may designate an affiliate.

Also, a company is not an affiliate if it meets any of the following criteria:

- Engages solely in holding the premises of the savings association.
- Engages solely in conducting a safe deposit business.
- Engages solely in holding obligations of the United States or its agencies or obligations fully guaranteed by the United States or its agencies as to principal and interest.
- Comes under control of the thrift as a result of the thrift's exercise of rights resulting from a bona fide debt previously contracted, but only for the period of time specifically authorized under applicable state or federal law or regulation. In the absence of a law or regulation, control may not exceed two years unless OTS grants an extension. Extensions may not exceed one year each and, in the aggregate, may not exceed three years.

If a transaction is not with an affiliate, then the TWA Rules do not apply. Subsidiaries of savings associations that are excluded from the definition of an affiliate are treated as equivalent to the association itself for purposes of the TWA Rules. Thus, an affiliate of the savings association is also an affiliate of that association's subsidiaries. As such, a transaction between a subsidiary of a savings association and the association's holding company or other subsidiaries of the holding company is also subject to the TWA Rules.

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. If you answer "yes" to any of the following questions, the transaction is a covered transaction and is subject to the standards in §563.41.

- Has the association or a subsidiary made a loan or extension of credit to an affiliate?

  Note: Certain less-obvious transactions may 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 thrift's personnel, premises, funds, or equipment without adequate compensation. Generally, if the institution conducts such transactions on an arms-length basis, consistent with how they conduct transactions with a non-affiliated party, OTS does not consider

transactions "de facto" extensions of credit or covered transactions. However, you should review all such transactions to determine whether §563.41 applies and, if so, whether the institution 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 or a subsidiary purchased assets, including assets subject to a repurchase agreement, from an affiliate? Do not include purchases of real and personal property that the FRB specifically exempts through regulation or order.

- Has the association or a subsidiary accepted securities that an affiliate issued as collateral security for a loan or extension of credit to any person or company?

- Has the association or a subsidiary issued a guarantee, acceptance, or letter of credit, including an endorsement or standby letter of credit, on behalf of an affiliate?

Congress enacted two specific prohibitions in the Home Owners' Loan Act (HOLA) that are more restrictive than sections 23A and 23B of the FRA. Congress added these prohibitions to reflect the fact that affiliates of savings associations can engage in a far greater range of activities than affiliates of banks, and can thus expose the savings association to greater risks. The TWA Rules prohibit two types of transactions:

- Purchasing or investing in securities of any affiliate other than in shares of a subsidiary.

- Making a loan or extension of credit to any affiliate unless such affiliate is engaged solely in activities described in HOLA 12 USC 1467a(c)(2)(F)(i) as defined in 12 CFR §584.2-2 (permissible bank holding company activities).

For the purpose of this restriction, a loan or other extension of credit includes a purchase of assets from an affiliate that is subject to the affiliate's agreement to repurchase the assets unless the affiliate meets the specific criteria outlined in 563.41(a)(3).

In determining whether HOLA prohibits a loan to an affiliate, you should attribute the activities of each subsidiary company to its parent company in a vertical chain up to, but not including, a controlling savings and loan holding company. However, loans to a "sister" thrift or bank are permissible regardless of the types of activities in which the sister thrift's service corporation engages.

Even if a transaction is not a covered transaction under §563.41, it may still be subject to the requirements of §563.42. In addition, some affiliate transactions may be exempt from §563.41.

Is the Transaction Exempt?

Although an affiliate transaction satisfies the definition of a covered transaction, an exemption may nevertheless apply. Exempt transactions are generally not subject to the quantitative or qualitative restrictions imposed on covered transactions. However, §563.41(a)(6) requires <u>all</u> covered and exempt transactions to be on terms and conditions consistent with safe and sound banking practices. The following transactions are exempt from §563.41:

- After January 1, 1995, any transaction with a savings association or a bank:

  — That controls 80 percent of the voting shares of the savings association;

  — In which the savings association controls 80 percent or more of the voting stock; or

  — In which 80 percent or more of the voting shares are controlled by the company that controls 80 percent or more of the voting shares of the savings association.

  Note: These transactions are subject to the low-quality asset provision.

- Making deposits in an affiliated bank, thrift, or affiliated foreign bank in the ordinary course of correspondent business, subject to any restrictions that OTS or FRB may prescribe by regulation or order.

- The granting of immediate credit to an affiliate for uncollected items received in the ordinary course of business.

- The making of a loan or extension of credit to, or issuing a guarantee, acceptance, or letter of credit on behalf of, an affiliate that engages solely in activities permissible for bank holding companies, provided the institution fully secures the transaction with one of the following:

  — obligations issued or fully guaranteed as to principal and interest by the U.S. or its agencies.

  — a segregated, earmarked deposit account with the savings association.

- The purchase of assets having a readily identifiable and publicly available market quotation and purchased at that market quotation.

  Note: To be eligible, the institution must establish asset value according to the market-at-large, such as stocks listed on a major stock exchange. Market quotations must appear regularly in a widely disseminated news source, such as the Wall Street Journal. Asset purchases based on Fannie Mae and Freddie Mac mortgage purchase quotations do not qualify.

- The purchase of loans on a nonrecourse basis from an affiliated bank or savings association subject to the prohibition on purchasing low-quality assets set forth in §563.41(a)(5).

- The purchase from an affiliate of a loan or extension of credit that the savings association originated and sold to the affiliate subject to a repurchase agreement or with recourse.

In addition to these exemptions, FRB issues interpretive rulings that may create additional exemptions from §23A. The FRB created an exception for certain loan purchases at 12 CFR §250.250. This exemption applies to a thrift's purchase from an affiliate of whole mortgage loans or participations, within the context of a specific proposed transaction or series of transactions, on a non-recourse basis, before the affiliate committed to make the loan. In such cases, the thrift must conduct its own independent evaluation of the borrower's creditworthiness before it commits to purchase the loans or participations.

OTS views as unsafe and unsound a blanket advance commitment by an association to purchase a set amount of loans not attributed to a specific proposed transaction unless the commitment is conditioned upon the loans complying with the TWA Rules. Also, the exemption does not apply where loan purchases by the thrift constitute the primary source of funding for the affiliate's lending operations or the funds alleviate the affiliate's working capital needs. To determine whether loan purchases represent an eligible participation arrangement or an ineligible financing transaction, you must assess other sources of credit or funding used by or available to the mortgage banking affiliate and the volume of purchases by the thrift in relation to the affiliate's overall production and profits. Further, the §250.250 exemption may not be available when the thrift invests a substantial percentage of its capital in loans originated by an affiliate.

If a transaction with an affiliate is covered under §563.41, but is not exempt, it is subject to the TWA Rules.

Does the Covered Transaction Meet Quantitative Restrictions?

Any covered transaction with an affiliate that is not exempt is subject to certain quantitative restrictions. Through a review of internal records, you should verify that the association's and its subsidiaries' aggregate amount of covered transactions are within both of the following quantitative limits:

- 10 percent of the association's capital stock and surplus with any single affiliate.
- 20 percent of the association's capital stock and surplus with all affiliates.

Institutions should attribute transactions with third parties in which the proceeds benefit an affiliate to that affiliate for purposes of calculating compliance with the quantitative restrictions described above.

The institution should value "hard" assets, such as building and office equipment at their cost, minus depreciation. The institution should include amortizing assets, such as loans, in decreasing amounts as they amortize. When assets purchased are subsequently sold, the institution should subtract them from the balance of its covered transactions with the affiliate from which the asset was purchased, and from the overall total of transactions with affiliates.

The institution should attribute the dollar amount of transactions with a subsidiary company to a parent company in a method similar to the manner described for activities above. For purposes of these restrictions, the institution should attribute transactions to each parent in a vertical chain, up to, but not including a controlling savings and loan holding company.

Does the Covered Transaction Meet Qualitative Restrictions?

Covered transactions are also subject to certain qualitative restrictions. A covered transaction may not include a low-quality asset and must be on terms and conditions consistent with safe and sound banking practices. A low-quality asset may include any of the following:

- An asset classified as substandard, doubtful, loss, or special mention in the most recent report of examination or inspection.
- 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 association may purchase a low-quality asset from an affiliate if the association, pursuant to an independent credit evaluation, committed itself to purchase the asset prior to the acquisition of the asset by the affiliate.

If a savings association lends or extends credit to an affiliate in a covered transaction, the transaction must be adequately collateralized in accordance with the requirements of §563.41(c). The thrift must obtain security for each loan or extension of credit to, or guarantee, acceptance, or letter of credit issued on behalf of, an affiliate. The collateral must have a market value equal to one of the following:

- 100 percent of the amount if the collateral is composed 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 Home Loan Bank or Federal Reserve Bank.
  - — A segregated, earmarked deposit account with the savings association.
- 110 percent of the amount if the collateral is composed of obligations of any State or political subdivision of any State.
- 120 percent of the amount if the collateral is composed of other debt instruments, including receivables.
- 130 percent of the amount if the collateral is composed of stock, leases, or other real or personal property.

You should verify compliance with these requirements through a review of the loan 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 to keep the percentage of the collateral value relative to the amount of the outstanding loan or extension of credit equal to the minimum percentage required at the beginning of the transaction. An affiliate cannot collateralize a loan or extension of credit, guarantee, acceptance, or letter of credit issued to, or on behalf of an affiliate, with a low-quality asset. Similarly, the affiliate cannot use securities issued by itself or another affiliate as collateral.

Section 563.42 of the TWA Rules contains additional qualitative provisions. All transactions covered under §563.41 are automatically covered under §563.42. In addition, §563.42 expands coverage to a broader base of transactions. Thus, some transactions that are not covered under §563.41, may in fact be covered by §563.42.

Compliance with the Provisions of §563.42

In addition to a review of affiliate transactions to determine compliance with §563.41, you must determine whether transactions comply with the restrictions of §563.42. To make this assessment, you should consider the following factors:

- Is the transaction with an affiliate?
- Does it involve a covered transaction?
- Does the transaction meet qualitative restrictions?
- Does §563.42 prohibit the transaction?

Is the Transaction with an Affiliate?

For purposes of reviewing a transaction under §563.42, the term affiliate has the same meaning given in §563.41, with one significant exception. The term affiliate does not include any bank or any savings association. This exclusion is tantamount to a type of "sister bank" exemption, but is broader than the sister bank exemption under §563.41 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 §563.41 because the 80 percent ownership criteria for the sister bank exemption is not met. However, the transaction may not be subject to §563.42.

Is the Transaction a Covered Transaction?

A covered transaction under §563.42 includes the following transactions:

- A covered transaction under §563.41.
- 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 thrift 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.

Also, the association or its subsidiaries should treat any transaction with any person as a transaction with an affiliate if the proceeds from the transaction are used for the benefit of, or transferred to, the affiliate.

Does the Transaction Meet Qualitative Restrictions?

If a transaction is a covered transaction, it must take place on terms and under circumstances, including credit standards, that are substantially the same, or at least as favorable to the association or its subsidiary, as those prevailing at the time for comparable transactions with nonaffiliated companies. In the absence of comparable transactions, the transaction must be on terms that, in good faith, would be offered to or would apply to nonaffiliated companies.

Does §563.42 Prohibit the Transaction?

OTS prohibits certain affiliate transactions altogether. Under §563.42, a thrift or its subsidiary cannot conduct any of the following transactions:

- Purchase, as fiduciary, any securities or other assets from the 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.
- Purchase or acquire, whether as principal or fiduciary, during the existence of any underwriting or selling syndicate, any security where a principal underwriter of the security is an affiliate of the thrift (unless a majority of the thrift's independent directors approves the purchase or acquisition of such securities before they were initially offered for sale to the public).
- Advertise or enter into any agreement stating or implying that the thrift is in any way responsible for the obligations of affiliates. Nor can the affiliate make any such representation in its advertising or otherwise.

Compliance with Recordkeeping Requirements

A thrift and its subsidiaries must retain records that reflect their transactions with any affiliate or any unaffiliated party 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 meet the following requirements:

- Identify the affiliate.
- Indicate the dollar amount of the transaction. Show that the amount is within the applicable quantitative limitations specified in §563.41 or that the transaction is not subject to those limitations.
- Indicate whether the transaction involves a low-quality asset.
- Indicate the type and amount of any collateral involved in the transaction and that the collateral complies in all respects with the collateral requirements in §563.41(c) or demonstrate that the transaction is exempt from these requirements.
- Demonstrate that the terms and circumstances of the transaction comply with the standards in §563.42.
- 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 Prior Notification Requirements

A savings association and its subsidiaries may have to notify OTS of transactions with affiliates if any of the following conditions are present:

- A de novo savings association that commenced operations within the last two years.
- An association or holding company thereof that has been the subject of an application or notice under Part 574 approved during the preceding two year period.
- A savings association in any of the following categories:
  - — Has a composite CAMELS rating of 4 or 5.
  - — Is not meeting all of its OTS regulatory capital requirements.
  - — Has entered into a consent to merge agreement, a supervisory agreement, or cease and desist order during the preceding two-year period, or is subject to a formal enforcement proceeding.

— OTS determines is in troubled condition and has so notified the association in writing. Additionally, OTS may restrict or prohibit transactions with affiliates when the thrift falls into one of the under-capitalized categories as defined in Part 565 (Prompt Corrective Action).

If notified in writing by OTS, a thrift must provide 30-days advance written notice prior to entering into any affiliate transaction. The notice should contain a full description of the proposed transaction. If OTS raises no objections during the 30-day period, the association or its subsidiaries may proceed with the transaction.

TRANSACTIONS WITH INSIDERS

In addition to the affiliate transaction restrictions, you must verify a thrift's compliance with standards for extensions of credit to insiders. Section 563.43 incorporates by reference application of the FRB's Regulation O (12 CFR Part 215) to federal savings associations, its subsidiaries 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.

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 §208.8(d).
- 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 thrift 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 over-

draft in a limited amount that is promptly repaid, as described in §215.4(e)).

- 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 or a similar transaction in which an association acquires assets and assumes liabilities of 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*.
- 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 are not considered loans, advances, or extensions of credit to the association of deposit; nor is the giving of immediate credit to an association upon uncollected items received in the ordinary course of business considered a loan, advance, or extension of credit to the depositing association.

General Requirements

Extensions of credit by a thrift or its subsidiaries to its insiders not specifically excluded by §215.3 are subject to the general prohibitions of Regulation O. Beyond direct extensions of credit to insiders, an extension of credit is made to an insider if the insider uses the proceeds of the extension of credit for tangible economic benefit or the insider receives the proceeds indirectly. There is an exception to the 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 non-insiders (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.

Regulation O generally requires that most extensions of credit to insiders, or extensions of credit for the tangible economic benefit of insiders meet the following criteria:

- 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.

The flow chart in Table 2, Insider Lending Restrictions Guidelines, presents insider lending transactions in a step-by-step manner consistent with the format outlined below. As we previously stated, you can use the Affiliate Transactions checklist (see Appendix A) to review insider lending transactions as well as transactions with affiliates.

Insiders

The Part 215 lending restrictions apply to executive officers, directors, and principal shareholders of the thrift and its affiliates. Insiders also include related interests of these executive officers, directors, and principal shareholders. Part 215 defines these terms which we summarize below.

It is important to note that Part 215 defines affiliate differently than §§563.41 and 563.42 as discussed earlier in this section under transactions with affiliates. Section 215.2(a) defines affiliate to include only the thrift'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 (Section 215.2(e))

Regulation O defines an executive officer as a person who participates or has the authority to participate in the major policymaking functions of the institution or its affiliate regardless of title. 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 presumes individuals with the following titles are executive officers:

- 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.

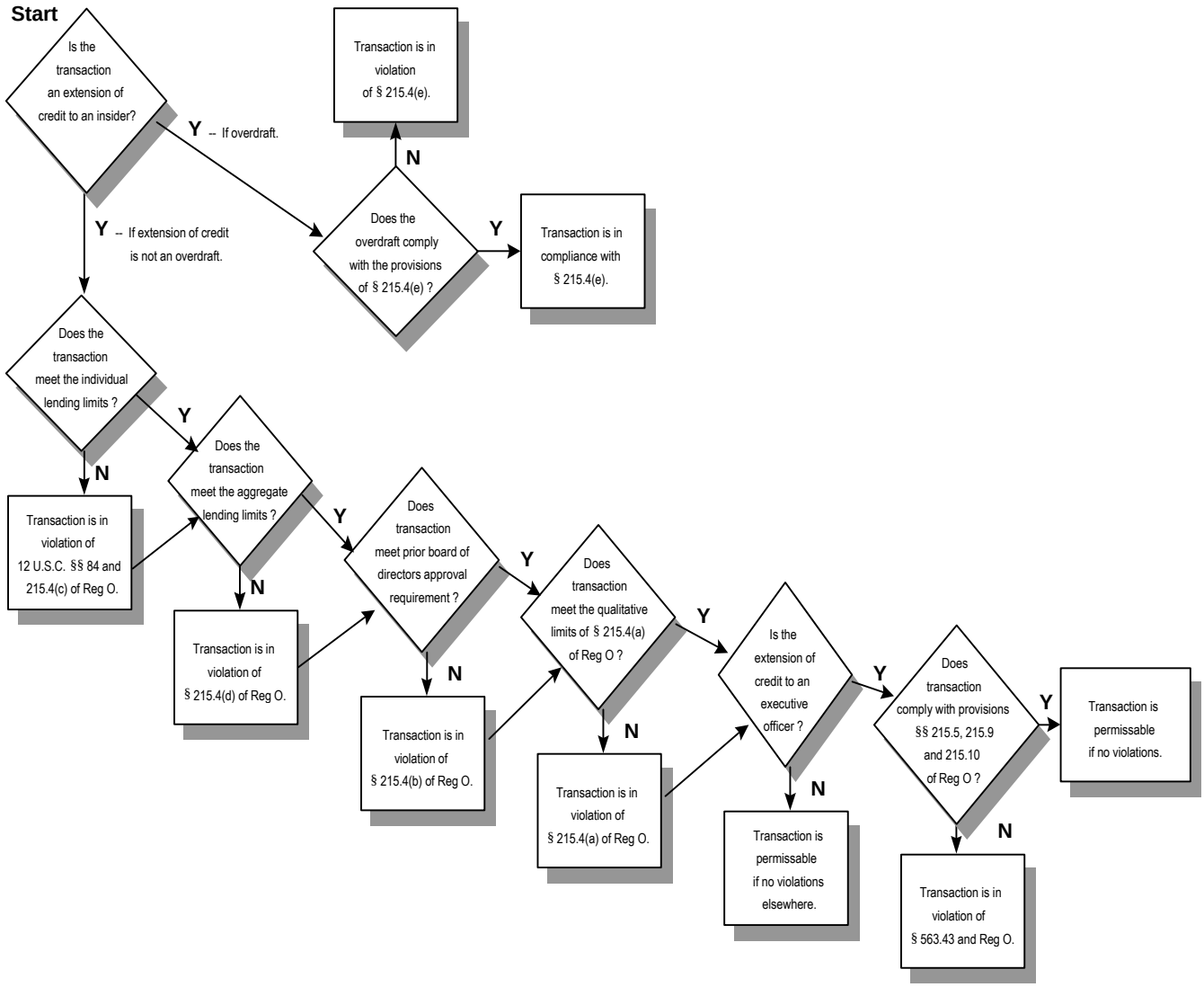
In some cases, the thrift may exclude individuals from the definition of an executive officer. The thrift can make the exclusion by name or by title in a list of individuals excluded from participating in such functions. The thrift can also make the exclusion by not including the officer in a list of persons authorized (by name or title) to participate.

Thrifts may exclude individuals presumed to be executive officers from the definition of executive officer if the following circumstances exist:

- A resolution of the board of directors or the bylaws of the institution or affiliate, excludes the officer from participating in policy-making functions of the association.
- The officer does not actually participate in policy-making functions of the association.

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:

Table 2
Insider Lending Restrictions



- A resolution of the board of directors or the bylaws of the association, excludes the officer 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 10 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))

Regulation O defines a director to include any person who the association designates as a director, or who performs duties as a director of the association regardless of the amount of compensation. The term director includes trustees. The term 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.

Regulation O provides an exception for extensions of credit to a director of an affiliate of an association. Unless otherwise subject by virtue of some other defining factor, (for example, the individual also serves as an executive officer of the association) directors of an affiliate 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 10 percent of the consolidated assets of the company that:
  - — controls the association; and
  - — is not controlled by any other company.

Principal Shareholder (§215.2(m))

Regulation O defines a principal shareholder to mean a person (other than an insured association) 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 10 percent of any class of voting securities of an association or affiliate. The institution should consider shares that a member of an individual's immediate family (as defined at 215.2(g)) owns or controls as held by the individual.

A principal shareholder does not include any company of which the association is a subsidiary. For example, principal shareholder excludes parent thrift holding companies.

Related Interests (§215.2(n))

Regulation O defines a related interest to include any company that an insider controls. It also includes a political or campaign committee that an insider controls, or the funds or services of a political or campaign committee that benefit that insider.

Restrictions on Extensions of Credit

Section 215.4 of Regulation O contains basically 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 such insiders, exceeds the association's unimpaired capital and unimpaired surplus. In other words, the aggregate amount of all transactions with insiders may not exceed 100 percent of the institution's unimpaired capital and surplus.

Aggregate Lending Limit — Small Institutions

Institutions 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 institution'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 institution meets or exceeds all applicable capital requirements.
- The institution received a satisfactory composite CAMELS rating in its most recent report of examination.

If the institution subsequently fails to meet fully phased-in 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 the following criteria:

- 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.
- Resulted 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 thrift's files or known to its officers.
  - — An officer of the thrift designated for that purpose by the board of directors of the thrift certifies in writing that the institu-

tion 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 insiders 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 its lending limits as described at §560.93. This limitation does not apply to an extension of credit by an association to its affiliates, instead, sections §§563.41 and 563.42 govern these transactions.

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 institution's unimpaired capital and surplus. An association may extend an additional 10 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.

The National Banking Act (12 USC §84(c)(1)-(10)) provides a list of 10 exceptions to the percentage ceilings for certain secured extensions of credit. The additional exceptions to thrift LTOB limitations contained in §5(u) of HOLA, are not available for extensions of credit to thrift 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, the following actions must occur:

- A majority of the 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.

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 institution 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.

Qualitative Treatment (§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, however, prohibit a thrift from making a "preferential" extension of credit to an insider if the thrift makes the extension of credit pursuant to an employee benefit or compensation program that is widely available to employees of the thrift and based on terms that are no more favorable than those offered to other employees. In addition, 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, unless the payment of funds meets one of the following criteria:

- Inadvertent overdraft(s), less than $1,000 in the aggregate, overdrawn for 5 business days or less and subject to the same fee charged to other customers (unless subject to a widely available benefit plan for all employees).
- 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 thrift's executive officers.* Thrifts may extend credit to an executive officer 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).
  - — 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 owned or expected to be owned by the executive officer also qualify for this category of residential loan, but only <u>one</u> loan may be attributed to this category of loans. (Institutions must attribute all extensions of credit for other purposes, even if secured by a residence, to the "other purpose" category 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(c)(4) limits to these same amounts, extensions of credit to a partnership in which one or more of the thrift'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 <u>each</u> officer of the thrift, individually, who is also a member of the partnership.

Any extension of credit to an executive officer must meet the following requirements:

- Reported promptly to the institution's board of directors.
- Comply with the terms and creditworthiness standards of §215.4(a) (i.e., not on preferential terms or involve more than the normal risk of repayment or other unfavorable features).
- Preceded by the submission of a detailed current financial statement of the borrower.
- Made subject to a written condition that the extension of credit will, at the option of the thrift, become due and payable at any time the officer becomes indebted to any other bank(s) or thrift(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. See Appendix B for a table of such requirements. 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 a thrift complies with the provisions that generally prohibit preferential extensions of credit to insiders of correspondent banks and imposes certain recordkeeping requirements. (See Appendix B.)

REFERENCES

United States Code (12 USC)

National Banking Act

§84 (c)	Lending Limits Exceptions

Federal Reserve Act

§371c	Banking Affiliates (23A)
§371c- 1	Restrictions on Transactions with Affiliates (23B)
§375a	Loans to Executive Officers (22(g))
§375b	Prohibitions on Insider Loans (22(h))

Home Owners' Loan Act

§1467a	Regulation of Holding Companies
§1468	Transactions with Affiliates, Insider Loans

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

§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 a Principal Shareholders
§563.200	Conflicts of Interest
§563.201	Corporate Opportunity
§574.4	Control
§584.2-2	Permissible Bank Holding Company Activities

Federal Reserve Board Regulations

Part 215	Regulation O (Insider Loans)
§225.28	List of Permissible Nonbanking Activities

Transactions with Affiliates and Insiders Program

Examination Objectives

Determine if transactions with affiliates and insiders are in regulatory compliance and not detrimental to the safety and soundness of the thrift.

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 other regulator(s) perform the review of scoping materials, obtain a written or verbal summary of the review(s) of items 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 noted 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.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

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
   - § 563.42
   - § 563.43 (which incorporates by reference the FRB's Regulation O at Part 215).

   Note: Appendix A, Transactions with Affiliates Checklist, provides step-by-step instructions. Appendix B, Summary of Regulation Reporting/Recordkeeping Requirements is also a useful tool to determine regulatory compliance.

6. Evaluate the association's documentation and recordkeeping to establish compliance with minimum standards.

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

Level II

8. Evaluate the extent and degree of influence of outside affiliations on the savings association.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

	Wkp. Ref.
9. From the review of information thus far, 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.	
10. Ensure that the examination 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

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Transactions with Affiliates and Insiders

Association	City	State	Docket #
Affiliate/Insider			
Description of Transaction			

Instructions: Use this Checklist to review all types of transactions with affiliates and insiders. Use the Checklist in conjunction with the regulations since the checklist does not include all of the definitions, etc. Follow the Checklist until you reach a **STOP**.

Is the transaction between the savings association or its subsidiary and an insider? (12 C.F.R. Section 563.43)

❑ Yes
Transaction may be subject to Section 563.43 (Sections 22(g) or 22(h) of the FRA)
➪ If the insider is a company, go to Part A
➪ If the insider is not a company, go to Part B

❑ No
Transaction may be subject to Sections 563.41 and 563.42 ➪ Go to Part A

PART A (563.41 and 563.42)

Note: Sections 563.41 and 563.42 parallel Sections 23A and 23B of the Federal Reserve Act.

1. Is the transaction between the association or its subsidiary and a company that conforms to the definition of an affiliate in Section 563.41(b)(1) and (2)?

❑ Yes
Transaction is with an affiliate as defined in Section 563.41
– If transaction is a loan ➪ Go to Next Step
– If transaction is not a loan ➪ Go to Step 3

❑ No
Transaction is not subject to the affiliate restrictions in Sections 563.41 and 563.42
➪ Go to Part B (563.43)

2. Does the affiliate engage only in activities permissible for bank holding companies as outlined in 12 C.F.R. Section 584.2-2?

❑ Yes
Transaction may be subject to Sections 563.41 and 563.42 ➪ Go to Step 4

❑ No
Transaction is a violation of Section 563.41(a)(3)
➪ STOP

3. Does the transaction involve the purchase of, or investment in, securities issued by an affiliate that is not a subsidiary of the association?

❑ Yes
Transaction is a violation of Section 563.41(a)(4)
➪ STOP

❑ No
Transaction may be subject to Sections 563.41 and 563.42 ➪ Go to Next Step

4. Is the transaction a "covered transaction" pursuant to Section 563.41(b)(7)?

❑ Yes
Transaction is a covered transaction as defined in Section 563.41(b)(7) ➪ Go to Next Step

❑ No
Transaction is not subject to the affiliate restrictions in Section 563.41 ➪ Go to Step 8

5. Is the transaction exempt pursuant to Section 563.41(d)?

❑ Yes
Transaction must still be consistent with safe and sound banking practices ➪ Go to Step 8

❑ No
Transaction is subject to quantitative restrictions ➪ Go to Next Step

6. Does the transaction meet the quantitative restrictions of Section 563.41(a)(1)?

❑ Yes
Transaction meets the quantitative restrictions ➪ Go to Next Step

❑ No
Transaction is in violation of Section 563.41 ➪ Go to Next Step

7. Does the transaction meet the qualitative restrictions of Sections 563.41(a)(5) and 563.41(c)?

❑ Yes
Transaction meets the qualitative restrictions ➪ Go to Next Step

❑ No
Transaction is in violation of Section 563.41 ➪ Go to Next Step

8. Is the transaction covered by Section 563.42(a)(2)?

❑ Yes
Transaction is subject to the qualitative restrictions of Section 563.42 ➪ Go to Next Step

❑ No
Transaction is not subject to Section 563.42 ➪ Go to Part B (Section 563.43)

9. Is the transaction prohibited by Section 563.42(b)?

❑ Yes
Transaction is in violation of Section 563.42 ➪ Go to Part B (Section 563.43)

❑ No
Transaction is in compliance with Section 563.42 ➪ Go to Next Step

10. Is the transaction on terms substantially the same as those offered to nonaffiliated companies?

❑ Yes
Transaction is in compliance with the qualitative restrictions of Section 563.42 ➪ Go to Part B (Section 563.43)

❑ No
Transaction is in violation of the qualitative restrictions of Section 563.42 ➪ Go to Part B (Section 563.43)

PART B (563.43)

Note: This part tracks the portions of 563.43 and Reg. O that are authorized by 22(h) of the FRA.

1. Is the transaction an extension of credit as defined by Section 215.3 of Reg. O?

   ❑ Yes
   Transaction may be subject to the restrictions of Section 563.43
   – overdraft ➪ Go to Step 13
   – any other extension of credit
   ➪ Go to Next Step

   ❑ No
   Transaction is not subject to the restrictions of Section 563.43 ➪ STOP

2. Is the extension of credit with an insider? (Do not consider exclusions or special provisions)

   ❑ Yes
   Transaction must be reviewed under Section 22(h).
   – executive officer ➪ Go to Step 3
   – related interest ➪ Go to Step 4
   – principal shareholder ➪ Go to Step 6
   – director ➪ Go to Step 9

   ❑ No
   Transaction is not subject to the restrictions of Section 563.43 ➪ STOP

Note: If the insider holds more than one position, follow directions for the first applicable step.

3. Is the individual excluded from the definition of an executive officer and was this exclusion appropriate? (Section 215.2(e))

   ❑ Yes
   Transaction is not subject to the restrictions of Section 563.43 ➪ STOP

   ❑ No
   Transaction may be subject to the restrictions of Section 563.43 ➪ Go to Step 9

4. Does an insider have control over a company as defined in Section 215.2(c)(1)?

   ❑ Yes
   Transaction may be subject to the restrictions of Section 563.43 ➪ Go to Next Step

   ❑ No
   Transaction is not subject to the restrictions of Section 563.43 ➪ STOP

5. Does this control relationship result in a rebuttable control determination?

   ❑ Yes
   The control determination may be rebutted
   ➪ Go to Step 7

   ❑ No
   Transaction is subject to the restrictions of Section 563.43
   ➪ Go to Step 9

6. Does a person or company meet the requirements of a principal shareholder? (Parent holding companies are excluded from the definition of principal shareholder.)

   ❑ Yes
   Individual/company is an insider
   ➪ Go to Step 9

   ❑ No
   Transaction is not subject to the restrictions of Section 563.43 ➪ STOP

7. Has the individual rebutted the presumption?

❑ Yes
Individual contends he is not in a control position ➪ Go to Next Step

❑ No
Individual is considered an insider ➪ Go to Step 9

8. Was the rebuttal accepted by the OTS?

❑ Yes
Individual is not considered an insider ➪ STOP

❑ No
Individual is considered an insider ➪ Go to Step 9

9. Does the transaction meet the individual lending limitations set forth at Section 215.4(c)?

❑ Yes
Transaction meets individual lending limitation ➪ Go to Next Step

❑ No
Transaction is in violation of Section 563.43 ➪ Go to Next Step

Note: Transactions with related interests should be aggregated with other extensions of credit to its insider.

10. Does the transaction meet the aggregate lending limitations set forth at Section 215.4(d)?

❑ Yes
Aggregate limitations are met ➪ Go to Next Step

❑ No
Transaction is a violation of Section 563.43 ➪ Go to Step 11

11. Did the transaction meet the board of directors prior approval requirements at Section 215.4(b)? (if unnecessary, check yes)

❑ Yes
Transaction meets prior approval requirements ➪ Go to Next Step

❑ No
Transaction is a violation of Section 563.43 ➪ Go to Next Step

12. Does the transaction meet the qualitative requirements of Section 215.4(a)?

❑ Yes
Transaction meets qualitative requirements
- executive officer ➪ Go to Part C
- director, principal shareholder or related interest ➪ STOP

❑ No
Transaction is a violation of Section 563.43
- executive officer ➪ Go to Part C
- director, principal shareholder or related interest ➪ STOP

13. Is the overdraft to a principal shareholder, or related interest of an insider?

❑ Yes
Transaction is permissible ➪ Go to Next Step

❑ No
Transaction may be subject to Section 215.4(e) ➪ Go to Next Step

14. Is the overdraft to an executive officer?

❑ Yes
Transaction is subject to Section 215.4(e) ➪ Go to Next Step

❑ No
Transaction may be subject to Section 215.4(e) ➪ Go to Step 16

15. Has the association excluded the individual from being considered an executive officer for purposes of Reg. O and was the exclusion appropriate? (Section 215.2(e))

❑ Yes
Transaction is permissible ➪ STOP

❑ No
Transaction is subject to Section215.4(e)
➪ Go to Step 18

16. Is the overdraft to a director?

❑ Yes
Transaction is subject to Section 215.4(e)
➪ Go to Next Step

❑ No
Transaction is permissible
➪ STOP

17. Has the association excluded the individual from being considered a director of an affiliate for purposes of Reg.O and was the exclusion appropriate? (Section 215.2(d))

❑ Yes
Transaction is permissible
➪ STOP

❑ No
Transaction is subject to Section 215.4(e)
➪ Go to Next Step

18. Does the overdraft meet the limitations of Section 215.4(e)?

❑ Yes
Transaction is in compliance ➪ STOP

❑ No
Transaction is in violation of Section 563.43 ➪ STOP

PART C (563.43)

Note: This part tracks the portions of 563.43 and Reg. O that are authorized by section 22(g) of the FRA (12 C.F.R. Sections 215.5, 215.9 and 215.10).

1. Is the extension of credit to an executive officer of the savings association?

❑ Yes
Transaction is covered by Section 22(g)
➪ Go to Next Step

❑ No
Transaction is not subject to Section 22(g)
➪ STOP

2. Has the association extended credit to the executive officer for the purpose of financing the education of the executive officer's children?

❑ Yes
Transaction is in compliance with Section 215.5(c)
➪ Go to Step 7

❑ No
Transaction may be subject to the limitations of Section 215.5(c)(4) ➪ Go to Next Step

3. Has the association extended credit to the executive officer to finance the purchase, construction, maintenance, or improvement of a residence of the executive officer *and* the extension of credit is secured by a first lien on the residence *and* the residence is owned (or expected to be owned after the extension of credit) by the executive officer?

❑ Yes
Transaction is in compliance with Section 215.5(c) ➪ Go to Step 7

❑ No
Transaction is subject to the limitations of Section 215.5(c)(4) ➪ Go to Next Step

4. Is the extension of credit secured as described in Section 215.4(d)(3)(i)(A) through (d)(3)(i)(C)?

❑ Yes
Transaction is in compliance with 215.5(c)
➪ Go to Step 7

❑ No
Transaction is subject to the limitations of Section 215.5(c)(4) ➪ Go to Next Step

5. Does the extension of credit, when added to all other extensions of credit to the executive officer (except those described in questions 2, 3 and 4) exceed the greater of 2.5% of the thrift's capital and unimpaired surplus or $25,000?

❑ Yes
Transaction is in violation of Section 215.5(c)(4)
➪ Go to Step 7

❑ No
Transaction may be in compliance with Section 215.5(c)(4)
➪ Go to Next Step

6. Does the extension of credit, when added to all other extensions of credit to the executive officer (except those described in questions 2, 3 and 4) exceed $100,000?

❑ Yes
Transaction is in violation of Section 215.5(c)(3)
➪ Go to Next Step 215.5(c)(4)

❑ No
Transaction is in compliance with Section 215.5(c)(4)
➪ Go to Next Step

Note: You should aggregate together the total amount of all extensions of credit:

- To partnerships in which one or more of the thrift's executive officers are partners, and either individually or together hold a majority interest.
- To the individual executive officers.

7. Has the executive officer met the reporting requirements and limitations of Sections 215.5(d)?

❑ Yes
Transaction is in compliance with Sections 215.5(d)
➪ STOP

❑ No
Transaction is in violation of Section 215.5(d)
➪ STOP

Exemptions/Exclusions/Special Provisions

_____

_____

_____

Violations Noted

_____

_____

_____

Regulation O Summary of Reporting/Recordkeeping Requirements

12 C.F.R. Section	Requirement
215.8	**Records of Institution** The thrift must maintain records that identify its insiders through an annual survey. Any recordkeeping method the institution adopts must include extensions of credit to insiders of the thrift's affiliates. The thrift can identify insiders of affiliates through an annual survey or by borrower inquiry method at the time the thrift makes an extension of credit. OTS may deem alternative methods acceptable. The thrift must also specify 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 must provide a written report to the thrift's board of directors within 10 days of becoming indebted to any other bank or thrift if the aggregate amount of the indebtedness exceeds $100,000 (or the greater of 2.5 percent of the thrift's capital and surplus or $25,000). The report must state the lender's name, the date and the amount, security and purpose of each extension of credit.
215.10	**Reports on Credit to Executive Officers** Thrifts must report in Schedule SI of its quarterly TFR all extensions of credit to its executive officers.
215.11	**Disclosure of Credit to Executive Officers and Principal Shareholders** Upon written request from the public, the thrift must make available a list of executive officers and principal shareholders and their related interests to whom the institution has an outstanding extension of credit that when aggregated with all other outstanding extensions of credit to that individual and their related interests equals or exceeds 5 percent of the thrift's capital and surplus or $500,000, whichever is less. The thrift does not have to disclose extensions of credit to any one person and their related interests that does not exceed $25,000. The thrift also need not disclose specific amounts of individual extensions of credit.

215.12 **Reporting Requirement for Credit Secured by Certain Bank Stock**

Executive officers or directors of institutions whose shares are not publicly traded must annually report to the board of directors any outstanding credit secured by shares of the thrift.

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 report to the board of directors outstanding indebtedness to correspondent banks of the thrift. The thrift must notify executive officers and principal shareholders of this requirement, make available a list of the correspondent banks, and maintain the reports for three years. Thrifts 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 thrift must make available the names of executive officers, principal shareholders and their related interests to whom a correspondent bank has outstanding extensions of credit to the individual and their related interests that equal or exceed 5 percent of capital and surplus or $500,000, whichever is less. The thrift does not have to disclose extensions of credit to any one person and their related interests that does not exceed $25,000. The thrift also need not disclose specific amounts of individual extensions of credit.