

INTRODUCTION

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

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

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

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

REGULATORY CONCERNS

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

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

DIRECTORATE RESPONSIBILITIES

The board of directors has the primary responsibility of establishing and maintaining an adequate and effective system of internal control. An effective

tive board generally has members who have financial or banking experience, and stature.

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

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

To oversee internal control and the external and internal audit function of an association, an audit committee comprised of outside directors (or at least a majority of outside directors) is desirable. Insured depository institutions covered by Section 36 of the Federal Deposit Insurance Act (assets total \$500 million or more), as implemented by 12 CFR § 363.1(a) must have an audit committee composed of only outside directors.

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

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

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

AUDITOR RESPONSIBILITIES

Internal Audits

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

External Audits

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

SAS No. 94, *The Effect of Information Technology on the Auditor's Consideration of Internal Control*, which amends SAS No. 55, provides guidance to auditors about the effect of information technology on internal control. It also establishes that an auditor should obtain an understanding of internal control sufficient to plan the audit and determine the nature, timing, and extent of tests to perform, including assessment of control risk. While this pronouncement places significant responsibility on the external auditor to look at internal control, the external auditor may

not extensively review controls over all areas of the association, and may use different levels of testing depending on the risk of a specific area.

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

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

When examining the communication of internal control matters noted in an audit, be aware that there is no standard form of communicating reportable conditions or material weaknesses to the audit committee. Once the auditor has chosen to discuss reportable conditions or material weaknesses, the auditor may do so either through a formal presentation to the audit committee, or informally, through conversations. The auditor may

also submit written reports. Generally, the auditor will document oral communications by appropriate memoranda or notations in the working papers.

INTERNAL CONTROL COMPONENTS

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

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

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring.

The Control Environment

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

Control Environment Assessment Process

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

Integrity and Ethical Values

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

Management Philosophy and Operating Style

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

Organizational Structure

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

Assignment of Authority

Assignment of authority includes policies relating to the following areas:

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

Human Resource Policies and Practices

Human resource practices send messages to employees regarding expected levels of integrity,

ethical behavior, competence, and conflict of interests.

Risk Assessment

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

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

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

The Risk Assessment Process

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

- Prevalence of external and internal factors that could affect whether strategic objectives are achieved.
- Effectiveness of systems used to manage and monitor the risks.
- Capacity of existing processes to react and respond to changing risk conditions.
- Level of competency, knowledge, and skills of personnel responsible for risk assessment.

Control Activities

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

The Control Activities Assessment Process

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

Performance Reviews

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

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

Information Processing

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

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

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

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

Physical Controls

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

- The physical security of assets, such as secured facilities.
- Access to books, and sensitive records and systems.
- Authorization for access to computer programs and data files.

Segregation of Duties

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

Information and Communication Systems

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

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

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

*Information and Communication Systems
Assessment Process*

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

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

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

Monitoring

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

The Monitoring Assessment Process

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

there are processes to ensure timely modification of policies and procedures, as needed.

ASSESSING CONTROL RISK

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

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

Assessing Control Risk at the Maximum

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

Assessing Control Risk at Less Than Maximum

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

- Conducting management inquiries.
- Inspecting documents and reports to review how staff performs controls.
- Observing directly how management applies the controls.
- Retesting how management applies the controls.

- Evaluating if management designs an effective internal control system to monitor and correct noncompliance.

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

Overall Assessment

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

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

LIMITATIONS OF INTERNAL CONTROL

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

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

We discuss each of these limitations below.

Judgment

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

Breakdowns

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

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

Management Override

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

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

Collusion

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

Fraud

Fraud is a broad legal concept, and involves intentional illegal acts that generally cause misstatement in the financial statements. Management bears the primary responsibility for detecting fraud. Internal control systems implementation is part of management's fiduciary responsibilities to prevent fraud and abuse by insiders. While the primary objective of an examination is the qualitative analysis of the association, fraud detection is certainly a goal when reviewing an association's internal control system. Recent problems concerning insiders at some associations have some commonalities. Potential red flags that could signal fraud include the following situations:

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

You should be aware of the potential warning signs of fraud and the examination and audit procedures that you should employ when warranted. If you encounter any red flags, you should bring the situation to the attention of the Regional Accountant. For more information, see 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 association is to assess the extent to which management has established internal control procedures and programs to identify and mitigate the association's internal control risks. In planning the examination, be aware of the following situations that may suggest that there is a breach in the control system that warrants attention:

- Management does not implement effective procedures to correct internal deficiencies noted in audit reports.
- Management scales back or suspends the internal audit function.
- The internal auditor has an operational role in addition to audit responsibilities. For example, the internal auditor reports through operating management and not directly to the board of directors or a committee. Ideally, the internal audit function should be under the board of directors or the audit committee, and the internal auditor should report directly to them. The extent to which the internal auditor reports to management may warrant attention to ensure that such reporting does not impair the independence of the internal auditor.
- The association's external audit firm lacks savings association or bank audit experience, or the auditors assigned have limited experience.
- The association enters new areas of activity without first implementing proper controls, or engages in new activities without experienced staff and appropriate controls in place.
- The association fails to provide adequate reports to the board of directors.

- The association does not have proper controls in high-risk areas.
- The association often deviates from board-approved policies with exception documentation.
- The association fails to effectively segregate duties and responsibilities among employees.

Level I Procedures

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

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

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

Management's Responses

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

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

Internal Audit Work Papers

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

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

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

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

Level II Procedures

Based on management's responses to questionnaires, or when an association does not have an effective system of internal audit, or when warranted based on examination findings, consider expanding the scope of the examination to include Level II procedures provided in the Internal Con-

trol Program. Also perform appropriate Level II procedures if the association outsources any significant activities and Level I procedures are insufficient to determine how the association controls the outsourced activity.

Issues that would require expanded procedures under Level II include:

- Concern about the competency or independence of internal auditors.
- No internal audit program is in place.
- Unexplained or unexpected changes occurring in the internal or external auditors, or significant changes occurring in the audit program.
- Inadequate controls in key risk areas.
- Deficient audit work papers in key risk areas, or work papers that do not support audit conclusions.
- High growth areas exist without adequate audit or internal control.
- Inappropriate actions by insiders to influence the findings and scope of audits.

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

- Account records are significantly out of balance.
- Management is uncooperative or poorly manages the thrift.
- Management restricts access to records.
- Significant accounting, audit, or internal control deficiencies remain uncorrected from previous examinations or from one audit to the next.
- Internal auditors are unaware of, or unable to sufficiently explain, significant deficiencies.
- Management engages in activities that raise questions about its integrity.

- Repeated violations of law affect audit, internal control, or regulatory reports.
- Other situations that you believe warrant further investigation.

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

OUTSOURCING RISKS

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

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

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

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

OTS expects associations to ensure that controls over outsourced activities are equivalent to those that the association would implement if they conducted the activity internally. The association's board of directors and senior management should understand the key risks associated with the use of service providers. They should ensure that an appropriate oversight program is in place to monitor each service provider's controls, condition, and

performance. See discussion of outsourcing in Handbook Section 355, Internal Audit.

REFERENCES

United States Code (12 USC)

Federal Deposit Insurance Act

- § 1831 Contracts Between Depository
 Institutions and Persons Provid-
 ing Goods, Products, or Services
- § 1831p-1 Standards for Safety and Sound-
 ness

Code of Federal Regulations (12 CFR)

- Part 363 Requirements For External Au-
 dits And Audit Committees
- Part 570 Appendix A, Interagency Guide-
 lines 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 Con-
 trol 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 Tech-
 nology on the Auditor's
 Consideration of Internal Control
 in a Financial Statement Audit
 (AU 319)