Office of the
Comptroller of the Currency

Washington, DC 20219

Office *of the* Comptroller *of the* Currency

Director's Toolkit

INTERNAL CONTROLS

A GUIDE FOR DIRECTORS

RESCINDED

September 2000

(reprint, September 2013)

This booklet is replaced by *Director's Reference Guide to Board Reports and Information* published November 2020.

Preface

Weak or ineffective internal controls, such as inadequate record keeping, external audit, or loan review, has caused operational losses in many banks and has contributed to the failure of others. Some of these cases involved insider fraud that could have been prevented or discovered through effective control mechanisms before the fraud resulted in loss to the bank. The Office of the Comptroller of the Currency (OCC) also has identified cases resulting in bank losses in which internal control weaknesses included improper and untimely reconcilements of major asset or liability accounts. In others, the bank did not institute or follow normal separation of duties between the physical control of assets and liabilities and the record-keeping functions involving those assets and liabilities.

Despite rapid changes in technology, the fundamental concepts behind effective internal controls remain the same. Effective internal controls form the foundation for a bank's system of risk management. They also safeguard bank assets; help the board and management guard against fraud and financial mismanagement; and ensure compliance with laws, regulations, and the institution's own policies.

To help the board and management meet their responsibilities, this pamphlet emphasizes the importance of establishing and maintaining effective internal controls. It also provides a description of basic control components and includes a series of questions that can assist directors and management in evaluating and improving their bank's internal control systems.[1] This guide supplements the OCC publications, *The Director's Book—The Role of a National Bank Director* and *Red Flags in Board Reports—A Guide for Directors*.

Internal Controls—Critical Components

The formality of any control system will depend largely on a bank's size and the complexity of its operations. Even though a community bank's operations are likely to be less formal and less structured, a bank's internal control system should be as effective as those at more complex and larger banks.

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO)[2] outlined five essential components of any internal control system.[3] The five components are:

1. control environment
2. risk assessment
3. control activities
4. accounting, information, and communication systems, and
5. self-assessment or monitoring

Each component is discussed below in more detail and is accompanied by a series of questions that address fundamental control activities. While this list is not all-inclusive, negative answers to these questions can help identify fundamental internal control weaknesses.

1. Control Environment

While each component is important, the first—control environment—is the foundation for all the others. The control environment reflects the overall attitude, awareness, and actions of the board and management concerning the importance of control activities. Overall, the control environment provides discipline and structure for the bank's entire operations.

The elements of a control environment include:

- Integrity and ethical values of personnel.
- Commitment to competence.
- Board of directors and/or audit committee participation.
- Overall influence of management's philosophy and operating style.
- Appropriate and adequate organizational structure.
- Clear assignment of authority and responsibility.
- Effective human resource policies and practices.

Control Environment—Questionnaire

Yes	No	
☐	☐	Does the board periodically review policies and procedures to ensure that proper controls have been instituted?
☐	☐	Is there a system in place to monitor compliance with policies and procedures and to report to the board instances of noncompliance?
☐	☐	When instances of noncompliance are reported, does the board take appropriate follow-up action and ensure effective action through testing?
☐	☐	Does management provide the board and the board's representatives complete access to bank records?
☐	☐	Are board decisions made collectively and not controlled by one dominant individual?
☐	☐	Does the board receive appropriate information from the bank's accounting, information, and communication systems to make informed and timely decisions?

- ☐ ☐ Does the board receive adequate information about the internal risk assessment process?
- ☐ ☐ Does the board review the qualifications and independence of the bank's internal and external auditors?
- ☐ ☐ Do the bank's internal and external auditors report their findings directly to the board or to the audit committee?
- ☐ ☐ Do the internal and/or external auditors periodically assess the adequacy of the bank's internal control systems?
- ☐ ☐ Are policies regarding the importance of internal control and appropriate conduct communicated to all employees?
- ☐ ☐ Do codes of conduct or ethics policies exist?
- ☐ ☐ Do audit or other control systems exist to periodically test for compliance with codes of conduct or ethics policies?

2. Risk Assessment

Risk assessment is the process the board and management use to identify and analyze risks that could keep the bank from achieving planned objectives. The assessment should help determine what the risks are, how they should be managed, and what controls are needed. Risks can arise or change because of circumstances such as:

- A change in the bank's operating environment.
- New personnel.
- New or revamped information systems.
- Rapid growth.
- New technology.
- New or expanded lines of business, products, or activities.

- Mergers or other corporate restructuring.
- Changes in accounting requirements.

Risk Assessment—Questionnaire

Yes	No	
☐	☐	Do the board and management appropriately evaluate risks when planning for new products or activities?
☐	☐	Do the board and management discuss and appropriately consider control issues when planning for new products and activities?
☐	☐	Are audit personnel or other internal control experts involved in control discussions when the bank is developing new products and activities?
☐	☐	Do management and the board involve audit personnel or other internal control experts in the risk assessment process?
☐	☐	Are technology issues considered and appropriately addressed?
☐	☐	Are there sufficient staff members who are competent and knowledgeable to manage current and proposed bank activities, and have they been provided with adequate resources?

3. Control Activities

Control activities include the policies, procedures, and practices established to help ensure that bank personnel carry out board and management directives. These activities help ensure that the board and management manage and control risks that could affect bank operating performance or cause financial loss. Policies governing control activities should ensure that bank officers who perform internal control functions in addition to their operational duties do not evaluate their own work.

Control activities are applied at various organizational and functional levels and include:

Operational performance reviews. These control activities include risk assessments and reviews of actual financial performance versus budgets, forecasts, and prior-period performance. In performing these reviews, the bank relates various sets of data—operational, risk related, or financial—to one another. The bank uses these comparisons to analyze the bank's actual versus projected performance to identify reasons for significant variances and to determine whether any specific bank activity should be adjusted.

Information processing. Banks perform a variety of control activities to verify the accuracy and completeness of transactions and to determine that they were properly authorized. Information systems control activities can be broadly grouped into two categories: general controls and application controls. General controls commonly include controls over data center operations, system software acquisition and maintenance, access security, and application system development and maintenance. These controls apply to mainframes, servers, end user workstations, and internal or external networks. Application controls apply to programs the bank uses to process transactions and help ensure that transactions are valid, properly authorized, and accurate.

Physical controls. Generally, these activities ensure the physical security of bank assets. They include safeguarding assets and records, limiting access to computer programs and data files, and periodically comparing actual asset or liability values with those shown on control records.

Segregation of duties. Banks establish segregation of duties by assigning different people the responsibilities for authorizing transactions, recording transactions, and maintaining custody of assets. Such segregation is intended to make it impossible for any person to be in a position to both perpetrate and conceal errors or irregularities in the normal course of his or her duties.

Control Activities—Questionnaire

Yes	No	
☐	☐	Do policies and procedures exist to ensure critical decisions are made with appropriate approval?
☐	☐	Do processes exist to ensure independent verification of an appropriate sample of transactions to ensure integrity?
☐	☐	Do processes exist to ensure ongoing and independent reconciliation of asset and liability balances, both on- and off-balance sheet?
☐	☐	Are key risk-taking activities appropriately segregated from reconciliation activities?
☐	☐	Do processes exist to ensure that policy overrides are minimal and exceptions are reported to management?
☐	☐	Does a vacation policy for critical employees ensure their absence for at least a consecutive two-week period?
☐	☐	Is there a system in place to ensure that duties are rotated periodically?
☐	☐	Is separation of duties and dual control over bank assets emphasized in the organizational structure?
☐	☐	Are systems in place to ensure that personnel abide by separations of duty?

4. Accounting, Information, and Communication Systems

Accounting, information, and communication systems identify, capture, and exchange information in a form and time frame that enable bank personnel to carry out their responsibilities. Accounting systems include methods and records that identify, assemble, analyze, classify, record, and report a bank's transactions. Information systems produce reports on operations, finance, risk management, and compliance that enable management and the board to manage the bank. Communication systems impart information throughout the bank and to external parties such as regulators, examiners, shareholders, and customers.

Accounting, Information, and Communication Systems—Questionnaire

Yes	No	
☐	☐	Do accounting systems properly identify, assemble, analyze, classify, record, and report an institution's transactions in accordance with GAAP?
☐	☐	Are the reports generated for operational, financial, managerial, and compliance-related activities sufficient to properly manage and control the institution?
☐	☐	Do accounting, information, and communication systems ensure that the bank's risk-taking activities are within policy guidelines?
☐	☐	Do all personnel understand their roles in the control system?
☐	☐	Do all personnel understand how their activities relate to others?
☐	☐	Do all personnel understand their accountability for the activities they conduct?

RESCINDED

5. Self-Assessment or Monitoring

Self-assessment or monitoring can provide oversight of a bank's control system performance. Management monitors internal controls to consider whether they are operating as intended and that they are appropriately modified when conditions change. Self-assessment, in the form of periodic evaluations of a department's controls by a person responsible for that area, is one type of oversight mechanism. For community banks, a clear and focused internal audit program can be a key defense against control breakdowns or fraud by providing independent assessments of the internal control system's quality and effectiveness.

Self-Assessment or Monitoring—Questionnaire

Yes	No	
☐	☐	Does the board review the actions management takes to deal with material control weaknesses and verify that those actions are objective and adequate?
☐	☐	Do audit reports contain sufficient detail?
☐	☐	Are audit reports timely enough to allow for resolution and appropriate action?
☐	☐	Does the board or audit committee approve the selection of key internal audit personnel?
☐	☐	Does the board or audit committee approve the overall scope of review activities (such as audit or loan coverage)?
☐	☐	Does the board or audit committee review results of audits?
☐	☐	Does the board or audit committee approve the system of internal controls?

- ☐ ☐ Does the board or audit committee periodically review audit or other key control systems?
- ☐ ☐ Is line management held accountable if they do not follow up satisfactorily or effectively on control weaknesses?

Other Resources and Publications Regarding Internal Control

AICPA Audit and Accounting Guide, "Banks and Savings Institutions."

AICPA Statement on Auditing Standards 55, "Consideration of the Internal Control Structure in a Financial Statement Audit."

AICPA Statement on Auditing Standards 78, "Consideration of the Internal Control Structure in a Financial Statement Audit: An Amendment to SAS 55."

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, Volume 1, *Executive Summary;* Volume 2, *Framework;* Volume 3, *Reporting to External Parties;* and Volume 4, *Evaluation Tools*.

The Institute of Internal Auditors, *Control Self-Assessment: Making the Choice*.

OCC Bulletin 99-37, Interagency Policy Statement on External Auditing Programs. (http://www.occ.treas.gov/ftp/bulletin/99-37.doc)

OCC Bulletin 98-1, Interagency Policy Statement on Internal Audit Programs and Internal Audit Outsourcing. (http://www.occ.treas.gov/ftp/bulletin/98-1.txt)

Basel Committee on Banking Supervision paper, "Framework on Internal Control Systems in Banking Organizations."

Comptroller's Handbook booklets: "Internal Control" (January 2001), "Community Bank Supervision" (July 2003), "Large Bank Supervision" (May 2001), and "Internal and External Audits" (April 2003).

---

[1] For a more extensive listing of internal control procedures, see the individual *Comptroller's Handbook* booklets such as those listed above.

[2] COSO is a voluntary private-sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.

[3] See COSO, *Internal Control—Integrated Framework:* Volume 1, *Executive Summary;* Volume 2, *Framework;* Volume 3, *Reporting to External Parties;* and Volume 5, *Evaluation Tools*.