FEDLINKS™
Connecting Policy with Practice

SUPERVISORY EXPECTATIONS FOR INTERNAL CONTROL FUNCTIONS

JULY 2013

Overview

Internal controls are processes that support an institution's efforts to attain objectives, maintain reliable financial and managerial reporting, safeguard resources, and minimize reputational and financial damage by preventing or detecting errors or irregularities. Internal controls promote compliance with laws and regulations as well as policies and procedures. Furthermore, internal controls allow banks to more effectively adapt to changing priorities, leadership, business models, and economic and competitive environments. Effective internal controls are one of the key foundations of a safe and sound financial institution with a strong compliance posture.

The purpose of this document is to describe 1) common elements of an effective internal control framework, 2) the process used by examiners to assess a bank's internal controls, and 3) common areas identified by examiners where banks could strengthen their control functions.

Expectations for Banks

It is the responsibility of an institution's board of directors and senior managers to consider the cost of implementing and maintaining strong controls versus the potential impact from the risk of lax or weak internal controls. Community banks are expected to have effective internal controls integrated with core processes that are adequate for the nature and scope of their businesses.

Community banks should adopt a recognized internal control framework that is appropriate for their needs and for safe and sound operations. The Committee of Sponsoring Organizations (COSO) of the Treadway Commission's *Internal Control--Integrated Framework* is an example of one such method that many banks have found to be useful[1]. Although this framework is used by multi-billion dollar financial institutions, it is flexible enough to work effectively at a bank with only $25 million in total assets as well.

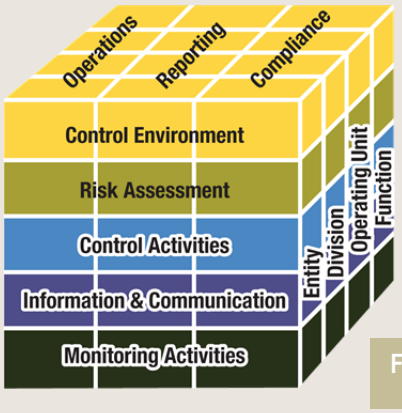

Figure 1

As depicted in Figure 1, the COSO framework includes five internal control elements. These elements can be tailored based on the size and complexity of the bank.

- ***Control Environment*** – The board of directors and senior managers are responsible for identifying the bank's key business strategies, objectives, and goals. Board members should tailor the control framework to influence the bank's philosophy, culture, and ethics with the goal of establishing and maintaining an appropriate control environment.
- ***Risk Assessment*** – The board of directors and senior managers should timely assess the risks at the entity level as well as the risks inherent in the activities and processes managed. After identifying the risks, the board of directors and senior managers should determine the bank's risk tolerance and establish risk measurement practices that are appropriate for their organization.
- ***Control Activities*** – Control activities can con-

[1] In May 2013, COSO issued an updated version of its internal control framework, which is depicted in Figure 1. The original 1992 framework will remain available during the transition period, which ends on December 15, 2014. Refer to www.coso.org for details.

sist of a mix of preventative and detective controls and can be manual or automated. Control activities are performed at all levels of the entity, at various stages within business processes, and across the technology environment. As risk exposures change, management should determine whether new and/or altered control activities are needed to manage the level of risk. Examples of key control activities are listed in Figure 2 on page 4.

- ***Information and Communication*** – Information required to successfully achieve the organization's control objectives should typically be stored in a management information system and disseminated to bank personnel as appropriate in a timely manner. Sensitive information also needs to be protected and controlled.
- ***Monitoring Activities*** – Monitoring of controls is often carried out within the business lines and by the audit function. Results of business line self-assessments and audit reviews should be communicated to the board and senior management in a timely manner. However, some smaller banks do not have an independent internal audit department. If a bank does not have an internal audit department, the bank should ensure appropriate review activities are built into operations, are ongoing, and are performed relative to the nature and scope of its activities. In addition to assessing the effectiveness of controls, monitoring activities often help institutions identify and manage areas with higher risk. For example, periodic fair lending assessments of loan denials and comparative file reviews are important to assist institutions in identifying, managing, and controlling their fair lending risk.

Examiner Assessment of Internal Controls

During each examination and as part of ongoing monitoring, examiners evaluate whether a bank's internal control function is effective. This begins with analysis of the organization's control environment and monitoring activities. As part of this assessment, examiners will determine whether work has been performed by the bank's functions (such as credit or compliance reviews and audit) that they might be able to use in their examination work. This information will assist in determining the examination scope. Although internal controls are broadly reviewed during each examination cycle, examiners will often focus the internal control assessment on one or more high-risk business activities, such as loan, wire transfer, or overdraft processing. Work performed often includes analysis and documentation of business processes and transaction flows to determine whether controls exist and are functioning properly. In addition, mitigating controls are typically considered and transaction testing is often conducted.

Observations on Internal Controls

What are some common observations made by examiners regarding areas where banks could strengthen their internal control functions?

- ***Risks and internal controls should be linked.*** For example, competitive pressures often prompt a reassessment of strategy, business processes, and product offerings. When a new business or product strategy is being considered, the board and senior managers should ask: What are the major risks of this plan? How much risk exposure are we willing to accept? Which laws, regulations, or supervisory guidance is applicable? What mitigating controls need to be in place to effectively limit these risks? How will we know if these controls are working effectively? By carefully considering risks as part of the planning process, controls can be built into the design, and ongoing monitoring can reveal when activities and results are missing their intended goals so that corrective actions can be more promptly initiated.
- ***Weaknesses in internal controls can be a sign of broader financial problems and vice versa.*** For example, during economic downturns in

which banks have struggled with asset quality problems, examiners have noted that it is not uncommon to find deficient internal controls in connection with significant asset quality problems at troubled banks.

- ***Built-in system controls are often more effective than manual controls.*** The use of system controls that eliminate the need for manual entries often improves compliance with both internal policies and regulatory requirements. For example, automated check holds that prefill hold notices and place holds on funds eliminate the potential for human error.
- ***Consumer fairness should be emphasized.*** Given the increasing regulatory focus on consumer fairness, the internal controls function should include activities designed to identify and mitigate unfair, deceptive, and abusive acts or practices. For example, a robust complaints monitoring program could help institutions identify and respond to bank practices that unfairly target or cause harm to consumers.
- ***Monitoring is more than information flow.*** Monitoring of the internal control system should occur on an ongoing basis. Evaluations should be performed regularly to determine whether the components of internal control are present and functioning. This might often involve automated processes built into operations that focus on deviations from established norms.
- ***Internal audit is not solely—or even primarily—responsible for internal controls.*** While internal audit might be involved in assessing risk and reporting on internal controls, audit is an independent assurance function rather than an internal control activity. Control activities are primarily the responsibility of management and should be embedded in business operations.

Inherent Limitations

The actions of bank personnel can limit the effectiveness of the established controls. For instance:

- ***Management Override*** – Even an institution with an effective internal control system may have a manager who is willing and in the position to override internal controls. There is a risk that a dominant official may overrule existing policies and procedures for illegitimate purposes with the intent of personal gain or to conceal financial results or compliance status. In addition to financial loss, the overrides may increase the potential for the unfair treatment of consumers.
- ***Collusion*** – When persons act collectively to perpetrate and conceal an action from detection, they can often alter financial data or other management information so that it cannot be identified by the control system.

Resources and Guidance

The Federal Reserve issued SR letter 95-51, "Rating the Adequacy of Risk Management Processes and Internal Controls at State Member Banks and Bank Holding Companies," dated November 14, 1995, which emphasizes the importance of sound risk management processes and strong internal controls. Specific internal control guidance is also found in the Federal Reserve System's Commercial Bank Examination Manual, Section 1010.1, "Internal Control and Audit Function, Oversight, and Outsourcing."

Policy statements on specific topics such as trading operations, structured finance activities, and audit functions also discuss internal control guidance. Community banks are encouraged to visit the Board of Governors of the Federal Reserve System's website to access related Supervision and Regulation letter guidance to further develop their understanding of supervisory expectations for internal controls.

Figure 2

Examples of Key Internal Control Activities

1. **Adequate safeguards over access to and use of physical and electronic assets and records**
   - Controlled access to documents, records, and assets is an institution's foremost defense against fraud and abuse. Both physical and electronic measures may be necessary to properly protect the bank's assets.
   - Automated processes and system controls often improve an institution's compliance with regulatory requirements. For example, built-in system controls may help identify when and which disclosures are required and may be set up to prepare the disclosures based on product parameters.
   - Other system controls can be used to help analyze large volumes of data. For example, automated tools, such as those used to identify suspicious transactional activity, may help institutions comply with Bank Secrecy Act requirements.
   - Administrative passwords should be controlled, and changes in records and computer system access control reports monitored regularly.
2. **Appropriate segregation and rotation of duties**
   - Persons with both access to assets and the ability to manipulate the related financial records may have the opportunity to misappropriate bank assets and/or conceal losses.
   - Systems should be in place to prevent or appropriately limit access to both assets and the related financial records.
   - Duties should be logically separated (whether manually or through automated applications) to reduce the risk of fraud and other inappropriate actions.
   - Employees in sensitive positions or risk-taking activities should not have absolute control over such areas.
3. **Restrictions on conflicts of interest**
   - Conflicts of interest create the potential that an employee will act in his or her own interest (or that of a related or affiliated party) rather than in that of the institution.
   - Systems should be in place to restrict employees from engaging in inappropriate transactions or transactions with affiliated or related parties.
4. **Appropriate establishment and enforcement of authority and risk limits**
   - Institutions should implement a process for reviewing compliance with approved limits, along with follow-up procedures for instances of non-compliance.
   - Approval and authorization requirements for transactions over certain limits ensure that management at the appropriate levels is aware of the situation and establish accountability.
5. **Adequate staffing levels and expertise**
   - An understaffed institution may find employees taking shortcuts to accomplish assigned tasks, resulting in breaches of controls and system overrides.
   - Internal control procedures are much less valuable when performed mechanically, without appropriate skepticism and judgment.
   - Employees should investigate issues identified and take appropriate action. Therefore, personnel must understand their roles in the control system, how their activities relate to others, and their accountability for the control activities they conduct.
   - In order to maintain appropriate levels of expertise, adequate training should be provided.