Implementing an Effective Internal Audit Function

By: Heidi Wier, CFSA & Sara McGinnis, CRCM, CAMS, CAFP

Contents

Introduction

An effective internal control structure is critical to the safe and sound operation of an institution. Effective internal controls safeguard assets, promote reliable financial and regulatory reporting, and help ensure compliance with relevant laws, rules, regulations, supervisory requirements, and institutional policies. An institution's senior management is responsible for establishing and maintaining an effective system of controls, including the implementation of official lines of authority and the appropriate segregation of duties.

Since 2004, NYSE-listed companies have been required to maintain an internal audit function to provide company management and key stakeholders, including the board of directors, audit committee, and shareholders, with ongoing assurance of the effectiveness of the company's control environment and risk management processes. Beyond the requirements for publicly traded companies, all the regulatory agencies including the OCC[1], Federal Reserve[2], FDIC[3], NCUA[4] and the CFPB[5] require strong internal controls and robust internal audit functions. In the case of the CFPB, an independent compliance audit is a required component of an effective CMS and one that the CFPB is focused on as it conducts its examinations. In addition, Government Sponsored Enterprises (GSEs) such as Fannie Mae[6] require approved sellers and servicers to "have internal audit and management control procedures to evaluate and monitor the overall quality of its loan origination and servicing processes, as applicable."

---

[1] Office of the Comptroller of the Currency https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/corporate-risk-governance/index-corporate-and-risk-governance.html

[2] Federal Reserve Supervisory Letter SL-16-11 Revised February 17, 2021 https://www.federalreserve.gov/supervisionreg/srletters/sr1611.htm

[3] Federal Deposit Insurance Corporation https://www.fdic.gov/regulations/safety/manual/section4-2.pdf

[4] National Credit Union Administration https://ncua.gov/regulation-supervision/manuals-guides/federal-consumer-financial-protection-guide/compliance-management/compliance-management-systems-and-compliance-risk

[5] "Compliance Management Review, General Principles and Introduction", CFPB Supervision and Examination Manual https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_supervision-and-examination-manual_2023-06.pdf

[6] Fannie Mae Selling Guide, Fannie Mae Single Family, published March 1, 2023 https://singlefamily.fanniemae.com/media/25041/display

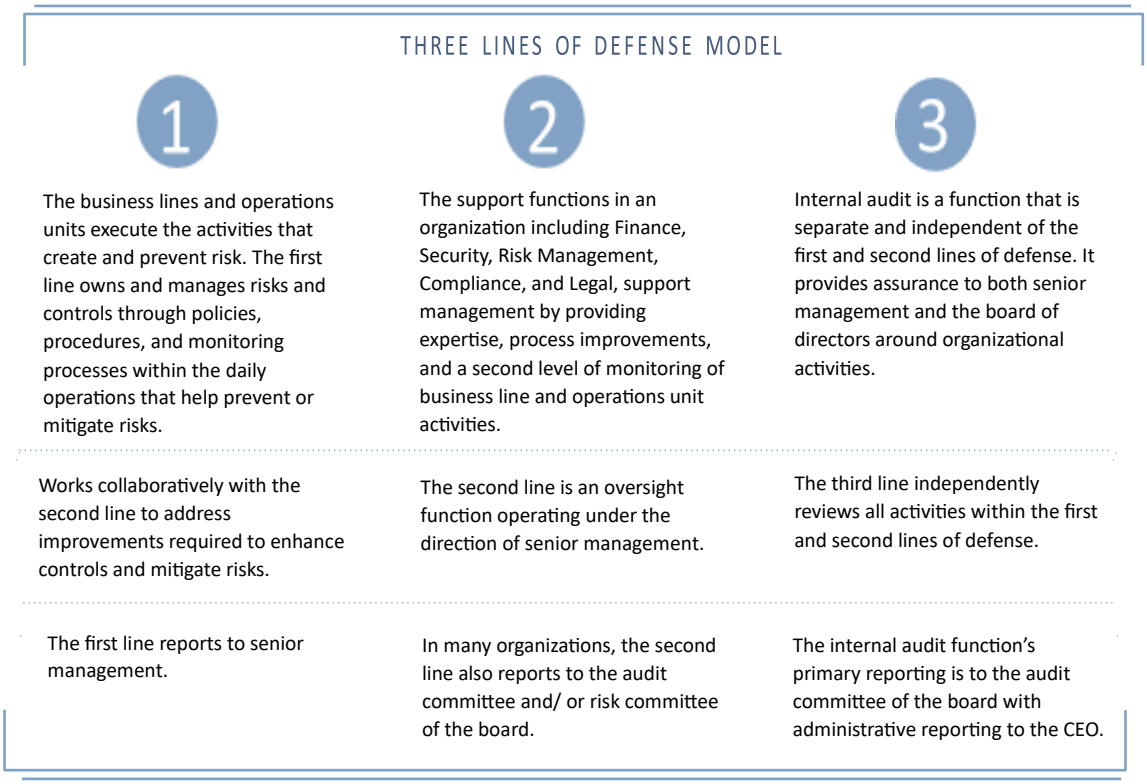
Corporate Governance

While the regulators and the GSEs may provide some guidance, the authority on internal audit for organizations across all industries is the Institute of Internal Auditors (IIA). The IIA is an international professional association and the recognized authority and acknowledged leader, advocate, and educator on internal audit. The IIA's International Professional Practices Framework provides guidance on internal audit effectiveness. Because publicly traded entities and banks have been required to have an internal audit function, these organizations have long been familiar with the IIA and consistently draw guidance from them. Other non-public companies and other non-bank financial services institutions may have utilized internal audits in managing their businesses, but others may be starting to fully develop an independent function.

The IIA defines internal audit as "an independent, objective assurance and consulting activity designed to add value and improve 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.[7]"

THREE LINES OF DEFENSE MODEL

A widely accepted practice of structuring an organization-wide control framework is based on the three lines of defense model. The model assigns duties and responsibilities for controls to segments of the organization as follows:



[7] The Institute of Internal Auditors – Standards and Guidance – International Professional Practices Framework (IPPF), www.theiia.org.

The first line of defense is the operational units or business lines. At this level, management should be able to determine if policies and procedures are correctly executed by the front line. A process of internal controls, self-monitoring, and correction should be built into the day-to-day functions to allow department managers and supervisors to ensure duties are being carried out in accordance with institution policies and procedures.

The second line of defense is typically comprised of the risk management function, which includes the compliance function. Generally, a management function, the second line provides guidance to the business units on how to design and structure controls to mitigate risks. The second line of defense typically performs ongoing and periodic monitoring and assists management with control enhancements as needed.

The third line of defense is the internal audit function. The audit function is a key element in a sound corporate governance structure and provides independent assurance to the board of directors and executive management about the effectiveness of internal controls and the state of compliance in the institution's operations.

INDEPENDENCE OF THE INTERNAL AUDIT FUNCTION

An effective internal audit function must be independent of and free from business unit influence and should not perform functions related to the daily operations of the organization. The chief audit executive should report directly to the audit committee of the board with unrestricted access to the board of directors and executive management. In many organizations, the chief audit executive reports administratively to the president or chief executive officer.

The internal audit standards of "independence" and "objectivity" may not yet be fully appreciated by institutions that are new to the concept of an internal audit function. Some mortgage companies, for example, believe the quality control unit or compliance team is also their internal audit function. While both the quality control and compliance units perform tests and provide feedback on performance, they are doing so as part of the first or second line of defense, at management's direction. An internal audit unit, in its role as the institution's third line of defense, operates independent of the first and second lines. In this example, internal audit will actually need to independently review the quality control and the compliance units as they are part of the audit universe.

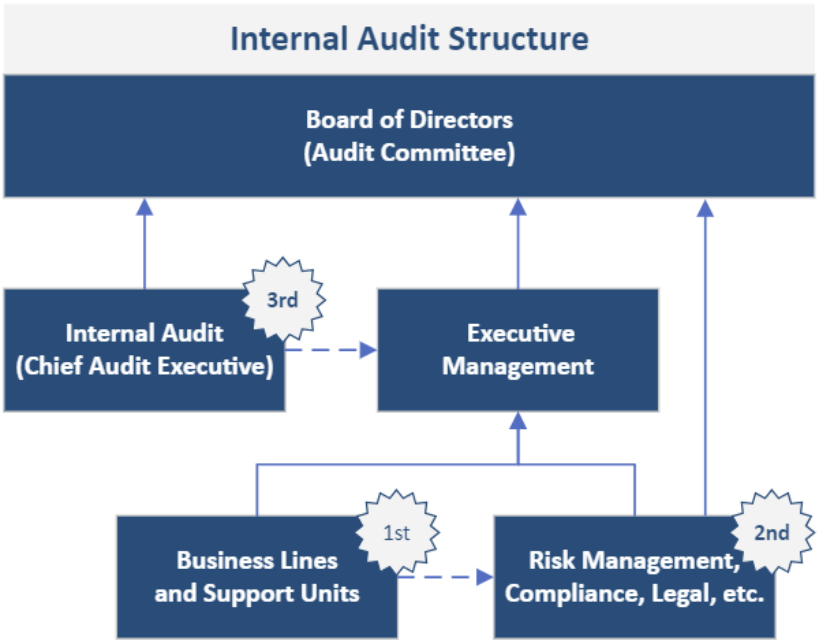
Structure of the Internal Audit Function

When deciding how to establish the internal audit function, management has some flexibility as the function should be commensurate with the organization's size and complexity. Some organizations may choose to engage external resources to supplement the function rather than staffing the entire function internally. The cost of the internal audit function grows with an institution's size and complexity; and companies should regularly evaluate which audits should be performed internally versus outsourced to a third-party service provider for added oversight and efficiency.

Some additional considerations when establishing an internal audit function include:

Accountability - While the duties of an audit function can be outsourced, accountability for the function and the results remains with management.

Expertise - Auditors must have the requisite knowledge and expertise in the area(s) to be audited.



Training – Up-to-date and ongoing training must be provided to ensure auditors maintain the necessary knowledge and expertise.

Independence - The audit function must be free from influence or bias in appearance and in fact. This is important when establishing an in-house audit department or if using a third-party firm. Third party firms should be engaged preferably by the designated chief audit executive or operations manager.

Vendor Management - If outsourcing the function, be sure to evaluate the external resource according to your vendor management program. Keep in mind that they are operating as an extension of your staff, and you are ultimately responsible for their actions.

The Internal Audit Process

Internal audit is a process of assessing risk, identifying controls to mitigate those risks, testing those internal controls for adequacy and effectiveness, and ensuring appropriate corrective action is undertaken when needed. Key steps in an effective internal audit function typically include the following:

Perform an institution-wide risk assessment to ensure all relevant risks have been identified, risk-rated, and properly addressed

An institution-wide risk assessment is the initial step in developing a comprehensive risk-based audit plan. While the risks to be assessed will vary by institution, typical risk categories include strategic, credit, compliance and legal, reputational, financial, technology, and operational risk. Assessing and prioritizing risk(s) should be done at least annually or more often when significant operational or product changes occur.

Non-depository mortgage bankers who sell loans to Fannie Mae are subject to a Mortgage Origination Risk Assessment (MORA) review. In these reviews, Fannie Mae has identified internal audit as an issue requiring management's attention.

Particular focus is on whether risk assessments performed include the areas of Quality Control, Originations, Closing, Funding, Underwriting, Servicing, and Secondary Marketing, as well as other areas pertinent to Fannie Mae's investor requirements. If internal audit is an area requiring improvement, be sure to allow sufficient time to properly address all of the components required for an effective internal audit function. Devoting sufficient time to this process will be the difference between an internal audit function that is quickly assembled to avoid criticism and an effective, worthwhile function designed to add value and improve an institution's operations.

Develop a risk-based, multi-year audit plan to assess whether controls are in place and operating as intended

The risk assessment will support development of a multi-year audit plan. A multi-year approach is recommended as areas identified as lower risk can perhaps be audited every two years. The audit plan should identify the frequency an area will be audited, with higher risk areas audited more frequently and at least annually. The multi-year audit plan should be evaluated and revised as necessary and at the conclusion of each risk assessment update.

To satisfy regulatory and GSE requirements, institutions will need to set aside sufficient time to perform the risk assessment prior to developing the audit plan. Estimating the audit plan without actually performing a comprehensive risk assessment may result in misdiagnosed or unidentified risks that end up costing the institution more in the long run.

Evaluate processes and controls to identify required improvements in the control environment

Internal audits will guide assessment and testing of policies, procedures, practices, and controls, and should be completed using a variety of methods including interviewing key personnel, reviewing policies and procedures, and detailed transactional testing. If issues or weaknesses are identified, the auditor should recommend practical solutions that address the root cause of the issue. In addition to addressing the root cause, internal auditors should evaluate the need for changes to procedures or controls, additional training, or enhanced monitoring. The internal auditor is a partner who has the best interest of the institution in mind. The goal of identifying practical solutions to issues and control weaknesses is to reduce risk and create a more efficient and effective institution, resulting in cost savings or additional profit. Internal audit is more than "checking the box."

Track and follow-up on previously identified control issues to ensure timely and adequate resolutions

When issues are identified, it is important that management take the appropriate corrective action to fully remediate the issue and the root cause of the issue. Internal audit should follow up on prior issues to ensure that appropriate, effective, and sustainable corrective action has been implemented and is effective.

In the course of its daily responsibilities, including follow-up on prior issues, it is imperative that the internal audit function have access to all institution records. Filtering information from internal audit signals lack of transparency. The purpose of an internal audit function is to provide management with independent and objective assurance that procedures and controls address the key risks an institution is facing. Anything short of providing full documentation creates red flags for regulatory agencies and investors.

Report findings to executive management or board of directors to ensure they are informed and provide oversight over the remediation process

Audit reports that include the scope, objectives, overall assessment, findings, and management's action plan for correction and validation of corrective actions should be provided to executive management. A summary for the board of directors by the chief audit executive will ensure presentation of all key findings and their resolutions. Executive management and the board are expected to provide active oversight and ensure appropriate remediation occurs. Meeting minutes should reflect discussion of the internal audit issues reported, related actions taken, and any further action that may be required.

When included in the institution's initiatives as an informed party, internal audit may provide insights on the operations and processes of the institution, which will result in more efficient and effective operational controls. They may also help business lines align with the board's strategy and expectations.

CONCLUSION

Institutions should embrace an independent and effective internal audit function that helps management promote good corporate governance by:

- Understanding risks
- Identifying opportunities for operational enhancements
- Reducing compliance errors
- Identifying and deterring potential fraud
- Limiting surprises
- Qualifying to sell to the GSEs

To take full advantage of this investment, management should ensure the function is comprised of individuals possessing the appropriate knowledge, skills, and discipline to execute the internal audit mission. Most importantly, for the organization to embrace the benefits that internal audit can provide, executive management and board support is imperative. Without that support, internal audit becomes a "check the box" activity whose full value will go unrealized to the organization and likely will not successfully keep it out of regulatory hot water.

ABOUT THE AUTHORS

Heidi Wier, CFSA
Managing Director – Regulatory Compliance, Internal Audit & Fair Lending

Heidi has over 30 years of experience consulting with mortgage companies, banks, credit unions, and fintech companies of all sizes on consumer protection laws and regulations. Prior to joining CrossCheck, Heidi held leadership positions in internal audit, mortgage operations, and compliance at Jefferson Wells International and Banc One Corporation, now JPMorgan Chase. She is a frequent instructor and presenter for mortgage and banking associations across the country and is also a published author on various compliance and audit topics.

Sara McGinnis, CRCM, CAMS, CAFP
Director – Regulatory Compliance & Internal Audit

Sara has extensive regulatory compliance and BSA/Anti-Money Laundering (AML) experience having worked in both consulting and industry over the past 25 years. She has provided regulatory compliance guidance to financial institutions ranging from small community banks to large, complex institutions. Her expertise includes having managed control audits in AML and fraud, risk and control assessments, loan compliance audits, and compliance monitoring reviews. Prior to joining CrossCheck Compliance, she held senior compliance and internal audit positions with United Services Automobile Association (USAA), U.S. Bank, Associated Banc-Corp, Johnson Financial Group (WI), and Wipfli LLP. She is a past instructor at the Wisconsin Bankers Association Real Estate Lending School and a published author on AML audits and flood compliance requirements.

Legal Disclaimer

This white paper is designed to provide general educational information in regard to the subject matter covered as of the date of this document and is not intended to be legal or regulatory advice for a specific financial institution. Questions regarding how this information applies to your financial institution should be directed to the authors or your legal counsel.