

MORTGAGE **Compliance** Magazine

Best Practices for Establishing a Cost-Effective Internal Audit Function

**Article by Heidi Wier
June 2016**

Best Practices for Establishing a COST-EFFECTIVE INTERNAL AUDIT FUNCTION

BY HEIDI WIER

The heightened regulatory focus on the mortgage industry is driving public and non-public mortgage companies to enhance their corporate governance structures by implementing effective internal audit functions. Publicly traded companies and certain other financial institutions have been required to maintain an internal audit function for years, but only in the last few years has the idea of implementing an audit function been getting significant attention in the mortgage industry.

As part of the aftermath of the 2008 financial crisis, the focus on internal audit functions has increased dramatically, not only by the Consumer Financial Protection Bureau (CFPB) and state regulators, but also by government-sponsored enterprises (GSEs) and other investors.

Lenders who sell loans to Fannie Mae are subject to a Mortgage Origination Risk Assessment (MORA) review, which includes assessing the adequacy and

effectiveness of the company's internal audit function. Fannie Mae also uses this MORA review process to evaluate all lenders who apply to become a Fannie Mae approved seller/servicer. As part of its recent MORA reviews, Fannie Mae has been citing many mortgage companies for lack of a sufficient internal audit function as an issue requiring management attention. And, although many



mortgage companies may get a MORA review before they will be examined by the CFPB, it is important to understand that the CFPB expects all its supervised entities to have an independent audit function.

CFPB EXPECTATIONS

The CFPB expects the organizations it supervises, both depository institutions and non-depository consumer financial services companies, to establish and maintain an effective Compliance Management System (CMS) to provide assurance to executive management and the board of directors that compliance policies, procedures, and internal controls are effective.¹ The CFPB expects mortgage companies to address four core pillars or control components:



- 1) Board and management oversight
- 2) Compliance program—including policies, procedures, training, and monitoring
- 3) Response to consumer complaints
- 4) Independent compliance audit

Note that the components include both auditing and monitoring, which are two separate and distinct functions, and the CFPB expects organizations to have both.

DEFINITION OF INTERNAL AUDIT

What is internal audit? 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 standards and effectiveness. According to the Institute of Internal Auditors (IIA):

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objective by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.²

Since publicly traded entities and banks have been required to have an internal audit function, these organizations have long been familiar with the IIA and regularly draw guidance from them.

THE DIFFERENCE BETWEEN MONITORING AND AUDITING

A common mistake when attempting to establish an internal

audit function stems from confusion between the concepts of monitoring and auditing. Monitoring is the testing that is done by the business units and risk functions to ensure business units are operating effectively. Monitoring includes quality control review and other quality assurance activities, and attempts to identify transactional, procedural, or training weaknesses so they can be remediated as part of an ongoing process improvement and internal control process. Monitoring is generally performed more frequently than internal audits and includes larger sample sizes to ensure wider and deeper coverage. Monitoring can also be completed by business unit or department personnel, as well as by support functions like compliance or risk management functions, as the requirement for “independence” does not apply to the monitoring function.

Internal audit, on the other hand, must be independent of the business units and free of any conflict of interest. Internal audit should have no operational responsibilities, and all departments, including compliance and other risk management functions, should be subject to audits by the internal audit function. Because of this requirement to be independent, it is imperative that independence be considered when determining the structure and reporting lines of the audit department. A common model to illustrate this concept is the three lines of defense model. ▶

THREE LINES OF DEFENSE MODEL

1

The business lines and operations units execute the activities that create and prevent risk. The first line owns and manages risks and controls through policies, procedures, and monitoring processes within the daily operations that help prevent or mitigate risks.

Works collaboratively with the second line to address improvements required to enhance controls and mitigate risks.

The first line reports to senior management.

2

The support functions in an organization including Finance, Security, Risk Management, Compliance and Legal support management by providing expertise, process improvements, and a second level of monitoring of business line and operations unit activities.

The second line is an oversight function operating under the direction of senior management.

In many organizations, the second line also reports to the audit committee and/or risk committee of the board.

3

Internal Audit is a function that is separate and independent of the first and second lines of defense. It provides assurance to both senior management and the board of directors around organizational activities.

The third line independently reviews all activities within the first and second lines of defense.

The internal audit function's primary reporting is to the audit committee of the board with administrative reporting to the CEO.

The model assigns duties and responsibilities for controls to segments of the organization as follows:

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

The second line of defense is typically comprised of the risk management support functions and 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 risk. The second line of defense typically performs ongoing and

periodic monitoring, and assists management with control enhancements as needed.

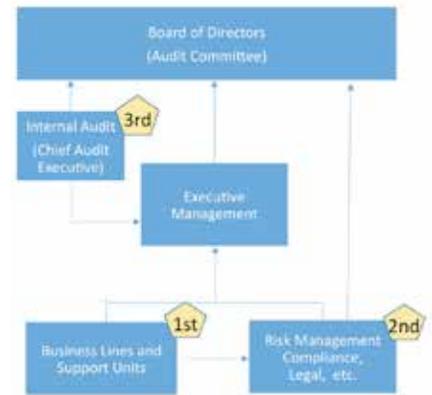
The third line of defense is the internal audit function. The audit function is a key element in a sound corporate governance structure and provides independent assurance to the board of directors and executive management about the effectiveness of internal controls and the state of compliance in the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

The internal audit standards of independence may not yet be fully appreciated by mortgage companies that are new to the concept of an internal audit function. Some mortgage companies believe the quality control department or compliance department is also the internal audit function. While both the quality control and compliance departments perform tests and provide feedback on performance, these are monitoring functions, and part of the first or second line of defense, at management's direc-

tion. An internal audit function, in its role as the company's third line of defense, operates independent of the first and second lines, and internal audit will actually need to include the quality control and the compliance departments in its audit universe.

STRUCTURE AND INDEPENDENCE OF INTERNAL AUDIT

When structuring your internal audit department, it is imperative that the function remains independent, free from conflict, and does not perform other functions related to the daily operations of the organization.



The chief audit executive (CAE) should typically report directly to the board of directors, or audit committee of the board of directors, and have unrestricted access to the board and executive management. In some cases, it may be necessary to have the CAE have 'dotted line' reporting to the president or CEO for administrative purposes. If your organization does not have a board of directors, then the audit function should report to the highest levels within the organization, such as the execu-

tive management committee. A common mistake, and one that is routinely criticized by regulators, occurs when the internal audit function reports to the compliance officer. This erodes the function's independence and creates a conflict of interest, as the audit department should audit the compliance area, to assure management that policies, procedures, and controls are in place and the organization is compliant with applicable laws and regulations.

Another common mistake is to assume that smaller organizations do not need to implement an audit function. Regulators expect ALL mortgage companies, regardless of size, to

have an effective audit function commensurate with its size and services. If it is not practical for an organization to establish an in-house audit function, management should consider using a third-party provider to meet its audit requirements.

THIRD-PARTY VENDORS

If outsourcing or co-sourcing the internal audit function, be sure to evaluate the external resource according to your vendor management program. And remember not all audit providers are created equal. You will want to be sure your vendor has an appropriate mix of mortgage operations, compliance, and internal audit experience. The most

relevant audit credentials to look for are Certified Internal Auditors (CIAs), Certified Financial Services Auditors (CFSAs), and Certified Public Accountants (CPAs). Keep in mind that any vendor is operating as an extension of your staff, and you are ultimately responsible for their actions.

AUDIT STAFF EXPERTISE AND TRAINING

When deciding how to staff 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 a company's size and complexity; and companies should regularly evaluate which audits should be performed internally and which audits, if any, should be outsourced to a third-party service provider for added oversight and efficiency.

Audit personnel must not only have the requisite knowledge and operational expertise in the area(s) to be audited, but also must have a strong grasp of internal audit standards and practices. Auditor expertise must be maintained with ongoing and sometimes specialized training. The IIA offers a variety of options for audit specific training.

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 include the following:

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

A company-wide risk assessment is the initial step in developing a comprehensive risk-based audit plan. While numerous methodologies with varying degrees of complexity exist for assessing risk, sometimes the best approach

is as simple as assessing and assigning each auditable entity a risk rating of high, moderate, or low, based on a series of risk factors to be evaluated. A typical risk assessment process includes the following steps:

- **Inventory potential audit areas** – Identify auditable areas, such as compliance, servicing, underwriting, secondary marketing, etc. Organizational charts can be helpful when determining the population of auditable areas.
- **Assess risk** - Gather existing policies, procedures, prior audit examination reports, strategic plans, financial reports, and related supporting information to identify risks and assess the control environment to mitigate those risks.
- **Assign risk rating** - Risk rate areas from highest to lowest. Be sure your risk ratings are uniquely defined.
- **Develop the audit plan** – Based on the risk ratings assigned, develop or adjust the audit plan to address the highest risk areas on a more frequent basis.
- **Update risk assessment as risks change** – Ideally, your risk assessment should be updated any time your risk changes, but at a minimum it should be updated annually. If you change strategies, add a new product, experience significant turnover, or have other changes that impact

your risk environment, consider the impact on your risk assessment, and make the appropriate changes.

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 higher risk should be audited more frequently, typically annually, and lower risk areas can be audited less frequently, perhaps on a biennial or even triennial basis, depending upon management's appetite for risk. The audit plan should identify the frequency an area will be audited, and should be evaluated and revised, if necessary, each time the risk assessment is updated.

Audit plans should be approved by the board of directors/audit committee and executive management each year. Significant changes in the plan or its scope should also be communicated to the board and executive management. Remember to document the approval of the plan in board or committee meeting minutes.

- **Executing the audit plan**

Executing the audits will include assessing 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 to address the root cause of the issue including changes to procedures or controls, additional training, or enhanced monitoring. The internal auditor should be viewed as a partner who has the best interest of the organization in mind. The goal of identifying practical solutions to issues and control weaknesses is to reduce risk and create a more efficient organization, resulting in more profit. Internal audit is more than “checking the box.” When executing the audit plan, consider the following:

- **Scope and sample selection**

– Audit scopes and sample selection should ensure adequate coverage of the audit area. The framework outlined by the IIA provides some guidance on sampling techniques, i.e. judgmental, or statistical samples.

- **Audit program development**

– While there are multiple sources for audit programs or test scripts, consider going directly to the source of the requirements. For example, the CFPB publishes its examination manual—it’s like having the test questions prior to the test.

- **Work paper documentation**

– The auditor’s work must be thorough and well documented. Each step should be detailed in a manner that allows it to be “replicated” or “re-performed” at a later date.

- **Management discussions**

– Be sure to discuss all initial findings and recommendations for improvement with management to ensure you have your facts straight and recommendations are practical given the business unit’s operations. There should be no surprises later in the process for either the auditor or the auditee.

- **Report issuance**

– Audit reports are typically first issued as a draft for management discussion and review. Management should be asked to provide written responses to recommendations that detail the specific corrective action to be taken to remediate issues and prevent recurrence. Final reports are then issued that include management’s written action plans for remediation.

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

When issues are identified, it is important that management take the appropriate corrective action to remediate the issue. This could range from making specific transactional corrections, to changing policies, procedures, practices, and retraining personnel if necessary. Internal audit

should follow up on prior issues to ensure that appropriate, effective, and sustainable corrective action has been taken. The designated audit committee or executive management committee should be provided on-going updates on status of prior internal audit findings which resulted in corrective actions.

In the course of its daily responsibilities, including follow up on prior issues, it is imperative that the internal audit function has access to ALL company records. For example, if a mortgage company operates in 20 states and has been examined by multiple state regulators, internal audit should have unfiltered access to and review all of those reports in their entirety. Filtering information for 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 a company is facing. Anything short of providing full documentation creates red flags to 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

Final audit reports that include the scope, objectives, findings, and management’s action plan for correction should be provided to executive management and summarized for the board of directors by the CAE to ensure all key findings are presented to ▶

the board. Executive management and the board are expected to provide active oversight and ensure appropriate remediation occurs. Board or committee meeting minutes should reflect discussion of the internal audit issues reported, related actions taken, and any further action that may be required. Keep in mind that regulators will also request any existing internal audit reports during the examination process to determine whether issues previously identified remain outstanding or have been remediated effectively.

BENEFITS OF INTERNAL AUDIT

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) established the CFPB, and with it, increased scrutiny over mortgage industry compliance with consumer financial laws became the norm. While the CFPB is focused on consumer regulatory compliance, other prudential regulatory agencies and the Department of Justice are focused on strategic, credit, operational and other compliance risks. As mortgage organizations embark on the new normal, it is important for management to understand the state of its control environment and where potential strategic, credit, operational, and compliance risks exist. Understanding your risks should be reason enough to implement an internal audit function; however, there are other good business reasons to make this investment.

- **No surprises** – Everyone sleeps better when you know what to expect. Internal audit's mission is to provide independent objective assurance to management and the audit committee regarding the effectiveness of the organization's risk management, control, and governance processes.
- **Understand risks** – A strong internal audit function should provide management with an understanding of the key risks the company faces and allow management to take the necessary steps to accept or mitigate those risks.
- **Qualification to sell to GSEs** – GSEs such as Fannie Mae require approved sellers and servicers to "have internal audit and management control systems to evaluate and monitor the overall quality of its loan production and servicing."³
- **Opportunities for operational enhancements** – Private companies with diverse product offer-

ings will find an effective internal audit function will not only assist with improving the control environment, but may also identify operating efficiencies and cost reductions, a desired benefit from any investment.

- **Reduce compliance errors** – Oftentimes, inadvertent operational errors result in technical compliance errors or errors that result in consumer harm. Internal audit's review of operational processes can help to prevent these types of errors, which may lead to costly customer remediation or litigation.

CONCLUSION

There are many good reasons why mortgage companies should embrace establishing an effective internal audit function, including good corporate governance and meeting regulatory requirements. 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. 



Heidi Wier, CFSA, is a managing director at CrossCheck Compliance. She is a regulatory compliance and internal audit executive with over 25 years of experience in the financial services industry. Heidi can be reached at: HWier@CrossCheckCompliance.com.

NOTES

¹ CFPB Supervision and Examination Manual – Version 2.0, www.consumerfinance.gov

² The Institute of Internal Auditors – Standards and Guidance – International Professional Practices Framework (IPPF), www.theiia.org

³ Fannie Mae Selling Guide, Fannie Mae Single Family, published March 29, 2016, page 5 (Eligibility) <https://www.fanniemae.com/content/guide/selling/index.html>