ABA Bank Compliance

SEPTEMBER | OCTOBER 2016

Compliance in 3D

The Second Line of Defense: Are the Stars Aligned?

BY LIZA WARNER, CPA, CFSA, CRMA

THE FIRST LINE OF DEFENSE includes the sales force, customer service, and all operational functions that support the sales and servicing of an institution's products and services. Since the first line is executing the institution's strategies and business objectives on a day-to-day basis, it is primarily responsible for effectively managing and monitoring compliance risks associated with those activities.

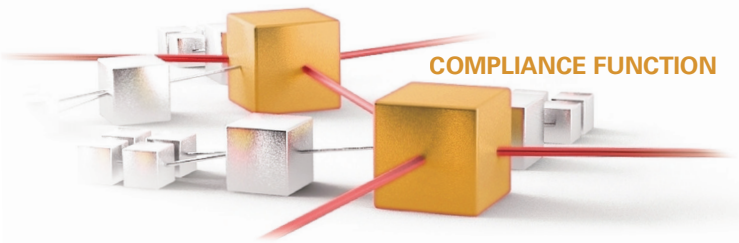
In a perfect world, the first line may have it covered and there may not be a need for a second line of defense. This scenario would require the first line to have detailed knowledge of all regulatory requirements, well-documented and implemented procedures to help guide activities, effective monitoring systems to detect instances of non-compliance, training programs at the ready to address areas requiring improvement, a change management process for systems and compliance procedures, and the ability to manage the onslaught of regulatory changes and their impact on day-to-day activities. However, things are rarely "perfect," least of all in dealing with today's regulatory environment, technological developments, and the pressure to sell and expand the customer base. In this imperfect world, the second line serves a very important role and purpose—supporting the first line of defense.

The second line is a risk management function reporting to the president or CEO, or in larger institutions, the chief risk officer. It is generally comprised of operational risk, third party risk, model risk, and compliance risk management programs. Each risk management program has a specific mandate, but they are also highly interrelated. The second line compliance function is responsible for oversight of the institution's compliance risk-taking activities by providing educational and interpretive guidance and by objectively assessing and monitoring first line compliance performance. It also reviews and reacts to issues that arise from the operational and third party risk management programs especially those that result in non-compliance with regulations or potential consumer harm.

Roles and Responsibilities of the Second Line Compliance Function

The OCC's September 2014 Guidance, *Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations*, and *Insured Federal Branches* describes the role and responsibilities of the second line, interpreted for the compliance function, as follows:

- **Primary responsibility and accountability for designing a comprehensive written compliance management program tailored to the compliance risk profile of the institution.** Responsibilities for compliance activities, monitoring, and reporting of issues must be clearly defined within the program and effectively operationalized within the compliance management system. This includes responsibilities for the first, second, and third lines of defense.
- **Perform ongoing compliance monitoring to identify and assess the institution's compliance risks and to determine corrective actions needed to**



strengthen compliance management. In addition to the monitoring activities expected within the first line of defense, the compliance function is also expected to conduct periodic enterprise-wide compliance monitoring. Results of second line monitoring will provide an independent view of compliance performance of the first line and will inform management of changes required to optimize the program. Significant issues identified by second line monitoring should be formally reported to executive management and the Board of Directors (or its risk or audit committee) to allow these stakeholders to fulfill their mandate within the compliance management system.

■ **Establish and adhere to the institution's compliance policies, procedures, and risk appetite statement.** The compliance function should work with senior management to develop and implement a comprehensive written policy that articulates its compliance risk appetite and is the basis for its compliance governance framework. The institution's compliance risk tolerances should be integrated into its overall risk appetite statement that addresses all major risk categories including credit, interest rate, liquidity, pricing, operational, strategic, reputation, and compliance risk. The statement should address qualitative components that describe a compliant risk culture and how the institution will assess and accept risks including risks that are difficult to quantify. For example, a qualitative statement related to training may state, "We provide our personnel with the tools and training needed to ensure the products and services we offer our customers comply with consumer financial regulations." It should also address quantitative limits. A corresponding quantitative limit may be, "All personnel are assigned compliance training applicable to their job and are required to complete 100% of the assigned training on an annual basis."

■ **Provide periodic reports of compliance performance to the CEO and Board of Directors or its designated committee.** Reports should include material risks of non-compliance, instances where the compliance function's assessment of risk differs from the first line, significant instances where the first line is not adhering to the compliance program.

■ **Direct access to the Board of Directors or its designated committee.** Compliance management, either through the chief compliance officer or the chief risk officer, has a responsibility to report instances where its assessment of compliance risk differs from that of the CEO, or where the CEO is not adhering to the compliance management program. Carrying out this responsibility would be extremely rare in a compliance conscious and transparent institution where management is committed to the compliance program.

■ **Develop, attract, and retain compliance talent.** In an environment where the competition for compliance talent is stronger than ever, it is imperative for management to work with human resources to manage compliance talent within all three lines of defense. The second line compliance function is relied upon by the institution to provide the requisite expertise and knowledge to support the enterprise wide program. To fulfill its role and responsibilities effectively, it must foster a culture that attracts and retains compliance professionals. At the top of most all compliance professionals' list is management's full support for the compliance program. A robust training and education program including participation in industry seminars and conferences is also expected. In addition to providing technical regulatory training, soft skills training including effective communication, presentation, and change management skills will help to make sure the messages do not get lost in translation or worse, ignored.

At its core, an effective and efficient compliance management system operates in a culture where compliance is "built into" processes and it is understood that it is a part of everyone's job. While there is no one regulatory definition of risk culture, the OCC Heightened Standards guidelines state that "risk culture can be considered the shared values, attitudes, competences, and behaviors present throughout the covered bank that shape and influence governance practices and risk decisions."

The industry has come a long way since the sole compliance officer who was responsible for all compliance. Over the years, and certainly since the 2008 crisis and with help from the regulatory agencies, institutions have recognized the necessity of strong risk management throughout an institution. While much has been done to implement the three lines of defense, there is more to do.

Structure and Approach

Institutions, both small and large, are still working on the best structure and approach for compliance management. In smaller institutions, the compliance function is naturally more integrated with the various departments in the first line. In many larger institutions, the first line is structured with its own mini-compliance function to help manage day-to-day compliance. Structured properly and with responsibilities clearly outlined, this latter approach can be effective. Without some guardrails, however, the activities may overlap or may be at odds with each other leading to confusion and unnecessary risk. Considerations for an effective relationship between the first and second line compliance structures include the following:

★ Senior management must establish and communicate expectations for a relationship that is collaborative and respectful. Everyone is in this for the same purpose, to protect the institution and ensure its customers are treated well and fairly.

★ Ensure responsibilities between the first and second lines are clear and create a partnership by completing a responsibility matrix. In its simplest form the matrix would include compliance responsibilities down the y-axis and the various first line functions and departments and the second line compliance function across the x-axis. For the compliance program and perhaps for large projects, the matrix should identify who is responsible, accountable, consulted, or informed (RACI) for each responsibility within the first and second lines. This approach is outlined by Mike Jacka and Paulette Keller in their book, Business Process Mapping: Improving Customer Satisfaction, and will help identify overlaps and gaps in responsibilities allowing for a more collaborative working relationship.

- **Responsible**—Individual or function who will execute the process.
- **Accountable**—individual or function approving completion of the process…the one "signing-off"
- **Consulted**—subject matter experts or counsel
- **Informed**—those who need to be kept apprised of the process

More than one role may be assigned.

★ Define who makes the final decision in situations when disagreements occur between the first and second lines of defense. A clearly outlined escalation process is necessary.

★ Oftentimes, first line "compliance personnel" report solely to the business line executive. Consider adding an indirect reporting line to the second line compliance function to help ensure consistency in carrying out the compliance mandate.

★ Schedule periodic meetings between first and second line compliance personnel, including first line management to facilitate communication and sharing.

★ Conduct joint training sessions on regulatory topics, non-regulatory topics such as change management, and teamwork sessions.

The saying about the stars becoming aligned doesn't actually refer to stars, but to planets—which, without a telescope, appear to be stars, but they move in orbits. Sometimes the orbits put two or more planets in alignment, one behind the other. It doesn't happen very often that the planets come together, thus it is considered fortuitous, perhaps portending something that perhaps was meant to be. Working together to align the planets and stars, the first and second lines of defense will establish a well-coordinated compliance program that effectively and efficiently identifies and mitigates compliance risk. Compliance with regulatory requirements should not be an afterthought; the ultimate goal is for the compliance function to be inherent in an an institution's cultural fabric. Only then, will everything be aligned. ■

ABOUT THE AUTHOR

LIZA WARNER, CPA, CFSA, CRMA, is a managing director at CrossCheck Compliance. She is a bank compliance and risk management executive with over 30 years of experience in the financial and professional services industries. Previously Liza was the chief compliance and operational risk officer for Associated Banc-Corp, where she was responsible for the management of the regulatory compliance and other risk management programs. Liza can be reached at **lwarner@crosscheckcompliance.com**. Phone # 262-649-2258.

Third Line of Defense: Internal Audit

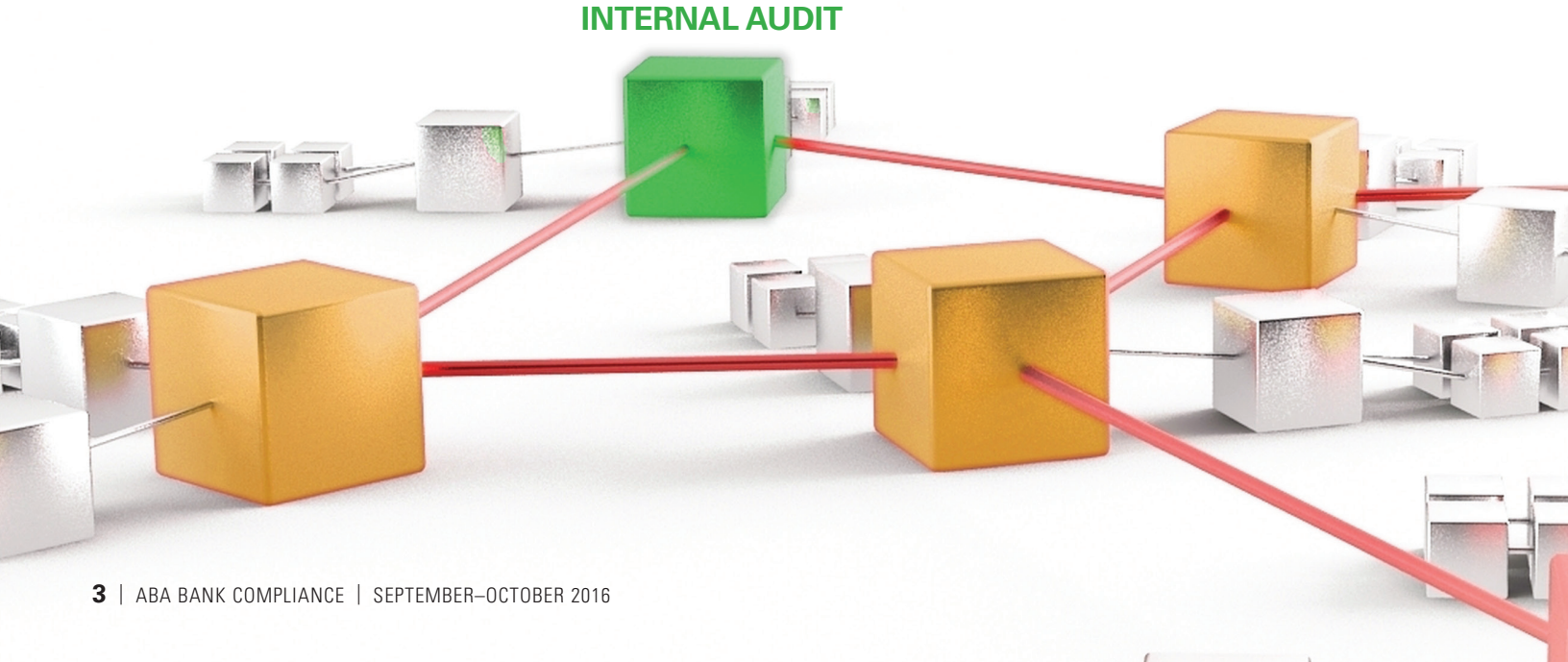
BY LIZA WARNER, CPA, CFSA, CRMA

OVER THE YEARS, as control environments and governance structures in financial institutions have matured, so has the role of internal audit – the third line of defense. What started as a need to "trust, but verify" has advanced to include that and more. In a fully operationalized three lines of defense model, the business lines and support functions effectively manage daily risks and the risk management and compliance functions monitor and help to optimize the control environment. The internal audit function assesses whether the first and second lines are effective, conducts its own independent review and testing, and reports its conclusions to management and the board of directors. Today's effective internal audit function (whether fully internal, assisted by external expertise, or fully outsourced) also can provide credible challenge and help ensure that the risks of today and tomorrow are appropriately addressed by the institution.

Management and the Board's reliance on internal audit to provide insight on the institution's risk and control environments are critical to their oversight responsibilities. An internal audit function is required for all publicly traded companies by the New York Stock Exchange Listing Requirements. Additional requirements for financial institutions have been added by the banking regulatory agencies. Generally, the regulatory agencies state that an institution should have an internal audit system that is appropriate to its size and the nature and scope of its activities. The audit function should provide senior management and the Board of Directors with information about the system of internal control so that management can understand the institution's risks and take necessary prompt, corrective action when indicated. In larger institutions a function comprised of internal audit professionals with various levels and types of expertise is commonplace. For smaller institutions implementing the function can be more difficult. Many institutions of all sizes find it necessary to outsource some or all of the audit function to maintain appropriate and fully trained staff.

Internal Audit

Since 1941, the Institute of Internal Auditors (IIA) has been the most recognized authority on the internal auditing profession. The IIA Standards and Guidance, which are often referenced by the regulatory agencies, define internal auditing 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 manage-



ment, control, and governance processes." More simply put, internal audit's mission is "to enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight."

One of the most common and acknowledged internal control frameworks is established by the Committee of Sponsoring Organizations (COSO). The COSO framework defines internal control as "a process, affected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

The five components of the framework are: the control environment, risk assessment, control activities, information and communication, and monitoring activities. These components are supported by seventeen principles to facilitate implementation of the framework and help an organization to achieve its operations, reporting, and compliance objectives. The regulatory agencies reference the COSO framework in various guidance publications. The OCC Heightened Risk Standards for Large Banks for one, closely aligns with the COSO internal control components and seventeen principles.

Implementing the Function

All institutions (smaller institutions in particular) are faced with issues of cost and organizational structure when implementing a function that meets both the internal audit mandate and regulatory expectations. Even if financial resources are available to support the function, finding individuals who meet the requisite mix of experience and expertise needed by the institution is not always an easy task. Internal auditors are expected to have good general business acumen, understand the institution's operations and its nuances, recognize an effective control environment, have the ability to assess the control environment, recognize inefficiencies in processes, diplomatically communicate issues to all levels within the institution, add value to the institution's strategic objectives, and attain an understanding of regulatory compliance requirements. Those dedicated to the profession typically hold professional certifications that demonstrate their knowledge and expertise. That is quite a list of competencies to fulfill.

Institutions have some alternatives on how the function can be tailored to the size, nature, and scope of its business, but cannot fail to have an effective audit function. There are important considerations when deciding how to staff the audit function, but a few are particularly worth noting. It is best for the institution to assign responsibility for the audit function to a senior level manager. That individual, in his/her internal audit capacity, should have the authority to manage the function, be independent of the business lines and support functions, provide assurance reports, and have unrestricted access to the Board of Directors or its audit committee. If an institution determines that it cannot support a full-time resource, or it requires additional resources to execute the internal audit plan, it may decide to engage qualified resources from outside the institution. When engaging a third party, management should consult the March 17, 2003 Interagency Policy Statement on the Internal Audit Function and its Outsourcing (Policy Statement) for related regulatory guidance. As we know, the activities can be outsourced, but the Board and management cannot transfer responsibility to a third party no matter what a formal agreement may stipulate.

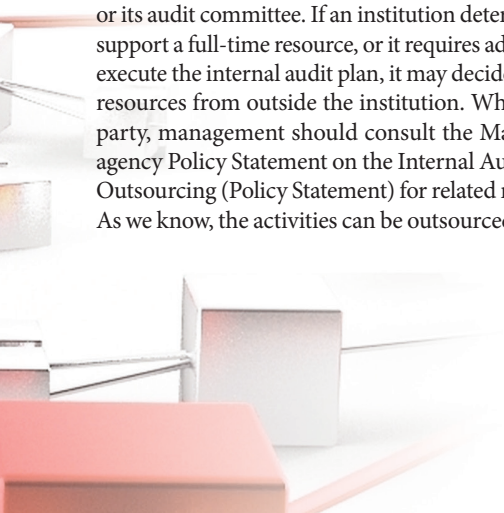
The March 2003 Policy Statement makes clear that for institutions outsourcing internal audit activities, senior management and the board of directors must continue to maintain responsibility for the system of internal control and for oversight of the internal audit function. In addition to the features of a sound internal audit function, the Policy Statement also outlines guidance around the use of third-party internal auditors and the prohibition on a public institution's outsourcing of internal audit activities to its external auditor under the Sarbanes-Oxley Act of 2002. In addition to its internal third-party risk management requirements, the institution should consider whether or not the third-party will conduct the internal audit activities in accordance with professional standards such as those outlined by the IIA. The standards address independence, professional proficiency, scope of work, performance of audit work, and management of internal audit.

At its core, an effective and efficient compliance management system operates in a culture where compliance is "built into" processes and it is understood that it is a part of everyone's job.

Unbiased Effective Challenge

As the "third line of defense," the internal audit function must be independent and objective in fact and appearance. As previously stated the audit committee should assign responsibility for the function to a senior member of management, carrying a title, responsibilities, and authority equivalent to other senior executives (for example, Chief Audit Executive (CAE)) who are not involved in daily operations and can bring forth unbiased opinions regarding the institution's control environment. Ideally the CAE should report directly to the audit committee on both audit issues and administrative matters such as resources, budget, performance appraisals, and compensation. In reality, many institutions have the CAE reporting directly to the audit committee on audit issues, but to the CEO or other senior executive on administrative matters. In some institutions, the CAE may report to another member of management such as the CFO. However, the audit committee, as it reviews adherence to the internal audit plan, should consider whether the CAE's objectivity and independence may be impaired as it relates to other functions under another senior executive's purview. One way to resolve potential conflict in the reporting structure could be to have an outside third party, who is independent of the other areas falling under the the common reporting structure conduct the internal audit of those areas.

The internal audit function is responsible for assessing risks in the control environment, preparing audit plans that address the risk areas, and executing audit programs according to the plan to determine whether or not internal controls are operating as management intended to help prevent errors, address errors and irregularities that are identified, including misappropriation of assets and potential for fraudulent activity, and evaluate the bank's compliance with regulations. The scope of the audit function's work encompasses the entire institution from front line activities andto back office support, to technology, finance, information security, business continuity, human resources.. It should also include an evaluation of the effectivenessof other functions, such



as the second line risk management and compliance functions. Internal Audit is expected to provide effective challenge and assist in identifying emerging risks such as social media, cyber security, politics, the economy, terrorism, etc.

Some questions to be answered in the audit area are:

- Are the checks, balances, and controls embedded within the first line of defense effective and working?
- Are the second line risk and compliance functions identifying where controls could be strengthened?
- Are issues identified by both the first and second lines being reported to appropriate levels of management and is corrective action appropriate and applied promptly?

Coordination with the First and Second Lines of Defense

Open and transparent communications between the internal audit function and the audit committee are vital to an effective third line of defense process. Also vital is the relationship between the rest of the institution and internal audit. While assurance is a primary responsibility and independence and objectivity are imperative, internal audit can add value by providing its expertise to other functional areas, including the first and second lines of defense. For example, along with other business and compliance considerations, internal audit's input on the risks and controls that should be addressed when changes occur (such as a new product, service, process, system, or regulation), will help ensure the changes are addressed with appropriate controls at the time of implementation. This level of coordination and collaboration can be very helpful to the institution, since doing things right the first time not only usually saves time and money, it may help avoid errors that increase reputation risk.

Management and the Board's reliance on internal audit to provide insight on the institution's risk and control environments are critical to their oversight responsibilities.

Of course care must be taken that the lines are not blurred between the second and third lines. In some cases, internal audit may be asked to assume responsibilities that are more appropriately handled by a business area or the second line of defense. This may be the case when the lines of defense are not fully implemented. The size or maturity of the institution or processes to implement a new risk requirement or regulation are also common factors that could put the audit function's independence at risk. If the lines are blurred, management and the board should be fully apprised and understand the potential impact such an arrangement could have on internal audit's independence and objectivity.

It Is About the Trust

Trusted relationships are essential for internal audit to be truly effective in meeting its mandate of enhancing and protecting organizational value, improving operations, and being considered a "trusted business advisor." Building relationships takes time and effort. Starting at the top, in addition to the audit committee, the CAE should participate in other board and management committees. Meetings should occur with business line management outside the audit plan schedule to listen to and understand the current state of operations and risks, including compliance-related considerations. Understanding how organizational value is created (both generally and specifically in your bank) will naturally help enhance and protect that value.

Meeting the Mandate

The days of simply checking a box and providing a list of exceptions, although still a part of the process, are long gone. Insight on why and how exceptions occurred, having the ability to identify alternative sustainable recommendations that improve the control environment, and effectively communicating in the language understood by the impacted areas, are becoming increasingly imperative in the audit function. Internal audit must also continuously evaluate its own processes and accept objective feedback to enhance the function, whether as part of an effective quality assurance and improvement program or as part of a cooperative corporate environment of continuous improvement.

Trusted relationships across all business lines, at all levels of the institution, and between all of the lines of defense will help facilitate transparent and goal-focused communications and actions. Internal audit will know when it has reached business advisor status when it is sought after by its partners as changes come about, issues surface, or when a question arises. When everyone in the institution instinctively thinks of how to do the right things in the right way to prevent issues rather than settling for simply detecting risks and with all three lines working together, success will be evident. ■

ABOUT THE AUTHOR

LIZA WARNER, CPA, CFSA, CRMA, is a managing director at CrossCheck Compliance. She is a bank internal audit, compliance, and risk management executive with over 30 years of experience in the financial and professional services industries. Previously Liza was the chief compliance and operational risk officer for a mid-size regional bank and has consulted with institutions of all sizes on their internal audit and compliance needs. She started her career in the internal audit function of what is now one of the largest national banks. She is a CPA, Certified Financial Services Auditor (CFSA), and holds a Certificate in Risk Management Assurance (CRMA). Liza can be reached at **lwarner@crosscheckcompliance.com**. Phone # 262-649-2258.