Compliance in 3D

The Three Lines of Defense and What You Need to Know
In a similar fashion, corporations have lines of defense to protect them against risks that could cripple their business operations or growth potential. The first line of defense consists of the front line staff who directly impact the activities that drive the company’s revenue, such as selling to customers or manufacturing goods. The second line is the risk management function (including compliance) that advises the first line and independently monitors and controls risk-taking. The third line of defense is the company’s independent audit function.

Since 2008, the three lines of defense framework for risk management have been outlined in pronouncements from the Federal Reserve Bank, the Basel Committee on Banking Supervision, and the Office of the Comptroller of the Currency (OCC). The emergence of the Consumer Financial Protection Bureau (CFPB) and its focus on fair and accurate treatment of consumers has placed an intensified focus on compliance management systems and the three lines of defense.

In September 2014 the OCC finalized Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches. This guidance includes minimum standards for the design and implementation of a risk governance framework for large national banks and minimum standards for the boards of directors overseeing those banks. The three lines of defense framework for managing all risks including compliance risk are intrinsic to the guidance. While the OCC standards were meant to apply to larger institutions, such as those with assets greater than $50 billion, the general premise and expectations have trickled down to smaller institutions as good risk management practices. They also seem to be considered by prudential regulators in their safety and soundness and compliance management system examinations and by the CFPB as they examine both bank and non-bank institution compliance management systems.

—LYN FARRELL, CRCM AND LIZA WARNER, CPA, CFSA, CRMA

Compliance Management Systems (CMS) are comprised of three lines of defense within an institution that include the business lines and support functions (first line), the compliance function (second line), and internal audit (third line). The concept of the “lines of defense” within financial institutions has its origins in military strategy. In a battle situation or one where soldiers are defending an important position, the troops that will face the enemy first constitute the first line of defense. The second and subsequent defense lines are troops that are farther back, closer to the home position. The second and third lines of defense only see action if the first line fails and the enemy gets through; the second line is then called upon to defend the home turf and, if it fails, the third line is activated.
Part of a Risk Framework
For banks, the first line of defense must be part of a risk framework that protects the bank from the risks of regulatory and legal violations. Without an operational and successful first line of defense, the bank is only able to find errors retroactively when compliance or audit groups find them later. By then, it’s too late to avoid their legal consequences. Finding mistakes retroactively is the risk management model under which banks have historically operated. The compliance group advised the lines of business on regulatory issues, and the lines of business either took the advice or not. If mistakes were made, compliance or audit found them, hopefully (but not always) before regulatory examiners did.

Imagine if other companies operated under that retroactive model. For example, if an automobile manufacturer did not incorporate risk management into its manufacturing processes, the workers on the assembly line might put together the parts of the car in a way that gave only cursory acknowledgement to government regulations governing auto manufacturing. For example, they might care about how the engine operated but not be too concerned that the catalytic converter was installed correctly, because, after all, the catalytic converter is only there because of government regulation. It doesn’t help the car run any better. In fact, it could impede the engine’s operation in favor of pollution control. So, assuming there was no first line of defense, the assembly line workers might or might not correctly assemble the catalytic converter and hope the second line staff, who are waiting at the end of the assembly line to monitor the process, will find and fix it before it leaves the plant to be sold. This would be a ridiculous process. No responsible manufacturer would operate this way, but it is the model banks have followed for much of the first 40 years of the consumer protection age.

One thing we now know: in today’s regulatory climate, the retroactive model does not work. It is a recipe for enforcement actions and consent orders. Any effective regulatory risk management framework has a working first line of defense at the forefront that is responsible for identifying and managing the risks of their own products and services. This is worth repeating another way. Compliance departments alone cannot keep the bank in compliance with regulatory requirements. They do not have the manpower or the authority.

First Line Principles
With that in mind, how does a successful first line of defense operate? Here are a few principles that should help to promote an effective first line of defense. In some cases these may need to be modified for smaller institutions.

1. Establish a clear structure of governance for first line personnel involved in compliance activities

The temptation is to give the staff involved in compliance activities for the front line some type of reporting line to the compliance group. The OCC and Basel documents make clear that the first line of defense should be completely independent from the second line risk management functions. First line compliance staff should report up to the line of business and their work outputs should primarily be targeted to the business leadership. Their performance reviews and compensation should be controlled within the line of business based on the goals and performance standards set by the business unit. There can be more leeway in this governance structure for some smaller institutions, although a completely independent first line is usually still preferable. In some cases, smaller institutions have so few staff members that it is best for the compliance group to have a more direct role in the first line of defense. This is especially true when the system is first getting established. However, even in these cases, the first line staff should have a dual reporting line, both to the compliance group and to the line of business.
2. Develop business-specific, compliance-related policies and procedures

The compliance group will always own the bank’s general compliance policies as well as the compliance risk framework, but the first line should have policies and procedures related to its specific compliance function, just as it does for functions related to lending and deposits. Procedures are especially important in the first line of defense. In jobs that are highly impactful on compliance risks (e.g., opening deposit accounts or interviewing loan applicants), having very specific procedures that will help steer the bank’s employees through customer interaction can prove vital to the bank’s compliance efforts.

3. Assess Compliance Risks

The first line of defense must identify and assess the regulatory risks within the business line. While the separate risk management group can advise the business units on the risks, the first line should own the identification and assessment process. This identification and assessment should interface with the compliance department’s risk assessment process. In some cases there may be differences of opinion of the levels of risks within a particular business line. The compliance group and the first line of defense are both equally responsible for the assessment of the risks, so they should reach a consensus on the level of inherent and residual regulatory risks throughout the line of business.

4. Monitoring and Testing

Typically the first line of defense assumes a monitoring, rather than a testing function. Like the quality controls built into the manufacturing process, the first line of defense is primarily responsible for day-to-day regulatory quality. Quality control monitoring should be a part of every transaction, such as post-consummation reviews of new deposit accounts and recently booked loans. With a rigorous monitoring system in place, the first line of defense should be able to find nearly all of its own regulatory problems before the risk management functions or auditors find them. Compliance monitoring processes may not be abundant within the first line of defense, but developing and executing them slowly, starting with high risk processes, is a good way to begin.

5. Metrics and Reporting

As in any aspect of running a business, line-of-business and product leaders should receive all reports and metrics necessary to effectively manage their businesses. Timely metrics on the regulatory compliance quality of the business unit contribute a necessary part of the data needed for good decision making. Data on transactional errors, compliance policy and procedure exceptions and customer complaints are all pieces of information that product leaders should use to run their businesses.

6. Issue Identification, Escalation and Remediation

Although historically the business units did not feel a responsibility to self-identify and escalate compliance issues, now these steps are integral to an effective first line of defense. In fact, a measure of the success of the lines of defense framework is that the first line finds most of the problems or issues rather than the second and third lines. The first line of defense needs processes for identifying errors and reporting them to the compliance group and to the appropriate governance committees. Remediation plans are another responsibility of the front line. This includes formulating remediation plans, having them approved by the compliance department, and executing the plans appropriately.

How the First Line Interacts with the Second Line

The first line of defense is independent of the second line, but it must coordinate monitoring and reporting activities with the compliance group and report remediation results to it. The first line should treat the second line compliance staff as a valuable advisory service and business partner that is essential to improving and maintaining the regulatory quality of its products and services. The bottom line is: it takes both an effective and engaged first and second line of defense to stave off regulatory trouble. If only one line is actively working, it will be hampered by the weakness of the other. Establishing an operational first line of defense takes time and effort, but the payoff comes in fewer regulatory findings and the cost savings found in the absence of examination findings, matters requiring attention (MRAs) and enforcement actions.

ABOUT THE AUTHOR

LYN FARRELL, CRCM, is a Managing Director at Treliant Risk Advisors, LLC, where she co-leads the regulatory compliance practice. Lyn is the author of the ABA’s Reference Guide to Regulatory Compliance and Law and Banking. She specializes in UDAAP compliance and compliance management systems. She has built UDAAP programs at large and medium-sized institutions. Formerly she has served as in-house counsel and chief compliance officer. She can be reached at farrell@treliant.com.

Endnotes

1. Review of the Principles for the Sound Management of Operational Risk, Basel Committee on Bank Supervision, October 6, 2014