Treliant®

From THE PULSE

FALL 2023

Management and Board as Lines of Defense

By Peter Reynolds

Peter Reynolds
Senior Advisor
Treliant

The three-lines-of-defense (3LoD) model is widely used by financial institutions to manage risk with the involvement of business units, risk management teams, and internal auditors. However, other lines of defense that receive less attention should come into greater focus—namely, a bank's executive management and board of directors.

These are, respectively, the fourth and fifth lines of defense. And in many ways, top executives and board members are the most critical roles in the defense model, since they establish an institution's risk culture. This article discusses challenges around the 3LoD model and the role that executive management and the board should play consistent with regulatory requirements and expectations.

Defining the Three Lines of Defense

The three-lines-of-defense model is defined similarly by regulators in the U.S. and Western Europe, consistent with the Institute of Internal Auditors' definition. The U.S. Office of Comptroller of the Currency (OCC) defines it as follows:

(continued on next page)

- "**First Line of Defense** is the frontline units, business units, or functions that create risk. These groups are accountable for assessing and managing risk … responsible for implementing effective internal controls, and maintaining processes for identifying, assessing, controlling, and mitigating the risks established with their activities …"
- "**Second Line of Defense** is commonly referred to as independent risk management (IRM), which oversees risk taking and assesses risk independent of the frontline units, business units, or functions that create risk. IRM complements the frontline unit's risk-taking activities through its monitoring and reporting responsibilities, including compliance with the bank's risk appetite. IRM also provides input into key risk decisions …"
- " **Third Line of Defense** is internal audit (IA), which provides independent assurance to the board on the effectiveness of governance, risk management, and internal controls …"

It is important to note that the loan review function, albeit not discussed here, is of comparable stature to the internal audit function and, depending on the institution, can be a third line of defense. Loan review officers perform a very critical and specialized activity, analyzing the bank's asset quality and its deployment and return of capital. When effective, the function's review results often mirror the findings in the annual Shared National Credit (SNC) process, a federal interagency effort for the evaluation and classification of lending.

3LoD Challenges

Banks have deployed the 3LoD model since the 1990s, benefiting from it regarding the safety and soundness of their institutions.

Some banks still struggle, however, to execute effectively on the 3LoD, especially between the first and second lines of defense. A significant challenge is that the execution of risk management tends to be siloed. Those responsible for activities within each respective line view the management of risk solely from their own perspective. The potential for redundancy of issues identified and activities performed can result in a level of inefficiency. This may also create gaps in coverage between the lines, with important risks not being managed effectively. Additionally, it can unintentionally absolve management and the board from maintaining their own defensive posture toward risk management.

Post the financial crisis of 2008, a significant amount of time and money has been and continues to be spent on risk management. Banks have organized and reorganized themselves in the hopes of driving more transparency, efficiency, and control coverage. Some banks for instance began to layer in additional lines of defense to try to achieve

Some banks still struggle to execute effectively on the 3LoD.

(continued on next page)

greater role clarity and assurance. Functions such as the controls group were created; however, their remit often overlapped with the operational risk function's. Similarly, the concept of 1.5 lines of defense once came into vogue, only to create confusion around activities performed by first and second LoD, especially in less mature risk organizations. Complicating these efforts has been confusion about organizational reporting lines, direct vs. indirect, for those supporting risk management.

The lines of defense can only be as effective as the support received from executive management and the board.

Through this all, it has not been clear where executive management and the board come out on the matter, and how they should engage to drive greater clarity, given their remit to uphold corporate and risk governance.

Illustration of Role Confusion

A recent and highly public example of risk management failure by a bank's top executives and board took place at Silicon Valley Bank (SVB). For eight months, there was not any chief risk officer (CRO) at the bank. There was an "Office of the CRO," an interim function, comprised of individuals who did not have the requisite skill set to take on such responsibility. Management was a member, which is an inherent conflict of risk independence. This arrangement prevailed as SVB's businesses continued to grow, introduce new products, and integrate an acquired business, First Boston, which had its own set of regulatory requirements different from SVB's core business. If not explicitly then implicitly the board, through its lack of action to replace the CRO, agreed with the arrangement.

What Needs to Change

Executive management and the board need to engage more rigorously in their respective risk management leadership roles in setting risk culture, while increasing their understanding of the practices of the 3LoD. In my experience as a regulator, industry practitioner, and now a consultant, management and the board generally lack a robust understanding of the first and second LoD's roles.

The lines of defense can only be as effective as the support received from executive management and the board. Having stated this, the lines of defense have to step up, too. The harmonization of risk among the first and second LoD can be uneven at times. A high-performing data-driven function like enterprise risk management needs to bring together risk findings by identifying risk anomalies, systemic issues, and trends across the enterprise, and then present them to executive management and the board. Bank leadership, in turn, must effectively challenge the lines of defense by asking probing questions to understand root causes and systemic and emerging risk.

Risk Culture

Risk culture is what differentiates a financial institution as it is established by executive management and the board. Culture can be measured. For instance, having a consent order or other form of regulatory sanction on a bank's record indicates a fractured risk culture. I once had a client who had received notice of over 200 matters

(continued on next page)

requiring attention (MRAs) and matters requiring immediate attention (MRIAs), with resolution of many of the issues overdue. That calls out a cultural problem for a bank its size, under $200 billion, and the general need for all institutions to have a risk communications and awareness program that propagates the subject and culture of risk.

A board's makeup should include individuals who understand both financial and non-financial risk management, with the regulatory acumen to address the subject of risk culture. Where there are knowledge gaps, regulatory guidance encourages retaining board advisors. Examples of poor risk culture abound in an industry largely driven by a bank's interest in being profitable, continually innovating, and maintaining a competitive edge over its peer group—while relegating risk management. As a former CRO, I once worked with a CEO who unilaterally decided to outsource private client information to a watch-listed country to save cost, which is clearly not evidence of a solid risk culture. Such action, albeit eventually reversed, created untenable risk for the time the information was outsourced and for whatever client information may have still been retained by the third party after the arrangement was terminated.

A board's makeup should include individuals with the regulatory acumen to address the subject of risk culture.

What Regulatory Issuances Say

Regulatory issuances such as the OCC's risk governance handbook are clear that executive management and the board are tasked from a corporate governance perspective with:

- Setting the bank's strategy, objectives, and risk appetite.
- Establishing the bank's risk governance framework.
- Identifying, measuring, monitoring, and controlling risks.
- Supervising and managing the bank's business.
- Protecting the interests of depositors and shareholders.
- Aligning corporate culture, activities, and behaviors consistent with the bank operating in a safe and sound manner, doing business with integrity, and complying with applicable laws and regulations.

Regulatory requirements and expectations are clear in their guidance, with the board playing a pivotal role in the effective governance of its bank. The board's accountability is to its shareholders, regulators, and other stakeholders. These "other stakeholders" extend to the employees of the bank, conferring responsibility to ensure that management is overseen and corporate values are established. Corporate governance sits squarely with the board, creating a risk governance framework to facilitate oversight and help set the bank's strategic direction, risk culture, and risk appetite. Talent management of top executives comes under its remit too, as the responsibility for having the right person in place to execute day-to-day operations inclusive of managing risk.

When composing a board, diversification of experience and skillset is critical. Board members' expertise should be in line with the bank's size, strategy, risk profile, and

(continued on next page)

complexity. Full access to all employees, regardless of position, if warranted, should be available to any board member. Direct interaction with staff and those holding roles of responsibility can help balance viewpoints and ensure that information going to the board is not filtered. This access will support the board in its responsibility for:

- Providing credible challenge to bank management.
- Establishing appropriate culture and tone at the top.
- Understanding the regulatory framework applicable to bank activities.
- Directing and overseeing an effective compliance management system (CMS).
- Confirming that the bank has a risk management system, including internal audit, that is commensurate with the bank's size and activities while also reflecting an understanding of material risks.
- Confirming that the bank has an effective system of internal controls.

If boards were to do this, they would truly be acting as a line of defense. But in my years of experience, I have witnessed few regulatory exams that challenge boards on how well they have executed on these responsibilities—especially the duty to promote risk awareness within a sound risk culture, one of the more critical roles.

> The CEO should be responsible for developing a written risk strategy with input from the business, independent risk management, and independent audit.

Internal audit may provide assurance to the board of the bank's risk control while remaining independent, but management tasked with day-to-day operations of the bank should be able to speak to the resolution of issues and to a risk strategy. Risk strategy needs to be aligned to the business' strategy and as such, management should understand and own each of these strategies. The audit function and the remaining lines of defense are there to support the safety and soundness of the institution, but it is management who ultimately owns the risk and is accountable.

One of the key activities for management is for the CEO to be responsible for developing a written risk strategy with input from the business, independent risk management, and independent audit. The expectation would not be for CEOs to write the plan themselves, but for them to oversee the writing of it, reach agreement on it, and own the finished product that is to be implemented. The strategic risk management plan should cover:

- Comprehensive assessment of risks both current and emerging, with the potential to materially impact the bank.
- An articulation of objectives that the strategic plan addresses.
- Clear timing on how often the plan is reviewed to account for internal and external changes impacting objectives, risk management, and control.
- Updating of the bank's risk profile consistent with plan reviews and taking action on the internal and external impacts they uncover.

If CEOs are close to their risk strategies, and plans are actively monitored, there will be less chance for surprise. It is not clear this always takes place, as evidenced by the number of enforcement actions and regulatory findings the industry experiences. Engagement from on top at times does not appear as robust as warranted.

If CEOs are close to their risk strategies, and plans are actively monitored, there will be less chance for surprise.

What's Next

Risk remains high: Financial services continue to evolve with disruptive innovation; non-bank financial service companies are taking command of critical services like payments; digitized and neo-banks are very much present; and regulation struggles to keep pace. Regulatory supervisors will need to renew the extension of their reach to address executive management and the board in more detail, including their behaviors in instilling a risk culture. Just as the three lines of defense can no longer be siloed, executive management and the board need to be called out as risk practitioners, too. This will become especially true for financial technology companies who have fewer dollars to invest in a 3LoD model than the well-established traditional banks. Management and board acumen for risk management will be called upon to compensate in these instances as regulation evolves.

The bottom line, regardless of bank or non-bank financial services: A more focused look at executive management and the board's risk management practices will need to be included explicitly in the lines-of-defense model.

Peter Reynolds

Peter Reynolds is Senior Advisor at Treliant. He is a global transformational risk and compliance executive with over 30 years of experience holding C-suite roles at Fortune 100 multinational financial services companies and Big 4 accounting firms. Peter is recognized for his deep risk expertise in banking and FinTech operations, including regulatory requirements and expectations and crisis management on a global scale. **PReynolds@treliant.com**

Treliant, Compliance, Risk Management, and Strategic Advisors to the Financial Services Industry, brings to you *The Pulse,* a quarterly newsletter offering insights and information regarding pertinent issues affecting the financial services industry. This article appeared in its entirety in the Fall 2023 issue. Other articles that appeared in this issue include:

- Does Your Organization Suffer from Compliance Complacency?
- Practical Considerations for the Merging of Two Banks
- Change Management in Financial Services: Compliance as Accelerant

To subscribe to our quarterly newsletter, *The Pulse,* visit **www.treliant.com/knowledge-center.**

Treliant®