Treliant®

From THE PULSE

SPRING 2024

The First Line of Defense Is Having Its Moment

By Karin Lockovitch and Laura Huntley

After a decade of attention on building out and maturing the second line of defense in risk management, the first line of defense is now getting its moment in the spotlight. The pressure is on, given regulators' heightened focus on operational resilience and first-line compliance—particularly with consumer protection rules. All of which has led to a significant increase in industry investment in first-line risk and control functions and a strengthening of internal control environments. This article analyzes the new focus on operations amid the ongoing evolution of the three-lines-of-defense model (LOD model) of risk management.

Background: Establishing the Three Lines of Defense

The LOD model emerged following the 2008 financial crisis as the recommended framework for effective risk management in financial services. While the design has continued to evolve, and variations in application exist, it remains today the most common model with the widest acceptance by banks and bank regulators.

(continued on next page)

WANT TO LEARN MORE?

We're presenting a complimentary webinar on June 4th at 2:00PM (ET). Register here to attend **"First Line Focus: Elevating Operational Compliance."**

The Institute of Internal Auditors (IIA) is credited with the original design of the LOD model. The IIA published a position paper titled "The Three Lines of Defense in Effective Risk Management and Control" in January 2013. The paper set forth the model for assigning and coordinating risk and control responsibilities across business functions, accelerating the elevation of the Chief Risk Officer (CRO) role. The IIA established the fundamentals of the model and described them in this way:

- **Operational Management as the First Line of Defense:** To own and manage risks—identifying, assessing, controlling, and mitigating them through the development and maintenance of effective internal controls.

  "Operational management naturally serves as the first line of defense because controls are designed into systems and processes under their guidance. … There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, inadequate processes, and unexpected events."

- **Risk Management and Compliance Functions as the Second Line of Defense:** To oversee risks— providing risk management frameworks; assisting operational management in establishing processes and controls to manage risks; identifying risks and emerging issues; providing guidance and training on risk management; measuring and monitoring risk appetite; and monitoring control effectiveness, risk levels, compliance, and remediation of deficiencies.

  "Each of these functions has some degree of independence from the first line of defense, but they are by nature management functions. As management functions, they may intervene directly in modifying and developing the internal control and risk systems. Therefore, the second line of defense serves a vital purpose but cannot offer truly independent analyses to governing bodies regarding risk management and internal controls."

- **Internal Audit as the Third Line of Defense:** To provide independent assurance—assessing the effectiveness of first- and second-line activities including risk management, compliance, governance, internal controls, and all business processes.

  "Internal auditors provide the governing body and senior management with comprehensive assurance based on the highest level of independence and objectivity within the organization."

The model suggested by the IIA was further promoted in a series of principles and guidelines set forth by the Basel Committee on Banking Supervision (BCBS) and the Financial Stability Board (FSB). In February 2013, the FSB issued a "Thematic

(continued on next page)

'Operational management naturally serves as the first line of defense because controls are designed into systems and processes under their guidance.' —IIA

Review on Risk Governance," which highlighted weaknesses in governance and risk management across the financial services industry. The review pinpointed the need for increased independence of risk management review and assurance, stronger management and board risk governance, elevation of the CRO role, and other remedies consistent with the LOD model. In July 2015, the BCBS authored the "Corporate Governance Principles for Banks," which reinforced the line-of-defense model principles and expanded upon the importance of the role of the CRO, principles for corporate governance, and responsibilities of the second line of defense, board of directors, and senior management.

In the past decade we have seen significant advancement in the design of the enterprise risk and compliance functions.

Since independent audit was not a new concept at this time, and already well adopted in the financial services industry, the focus of institutions implementing the LOD model in the years since has been on building and strengthening the second line of defense. In the past decade we have seen significant advancement in the design of the enterprise risk and compliance functions including substantial elevation in the level of expertise and seniority of the CRO and Chief Compliance Officer (CCO) roles.

Challenging the 3-Line Model

Fast forward to 2019, when rumblings about weaknesses in the LOD model were getting louder and starting to drive change. Challenges to the efficacy of the model included:

- Limited guidance regarding interaction and engagement across each line of defense;
- A higher adoption of the model for non-financial risk disciplines (e.g., regulatory compliance) than for financial risks (e.g., capital, liquidity, interest rate);
- A perceived lack of adaptability of the LOD model to suit changing institutional priorities, maturity, and business models;
- The nature of the LOD model as overly detective and reactive versus proactive and contribution-oriented;
- Insufficient attention to the appropriate coordination and communication across the lines; and
- Ambiguity and variability in how banks delineated roles and responsibilities across the first and second lines, which created redundancies, inefficiencies, conflicts, and inconsistencies in risk appetite interpretation and risk accountability.

Evolving the 3 Lines

Contributing to this noise has been the emerging focus by policy-makers and regulators on the operational resilience of banks, as they have been evolving through rapid technological innovation, a significant increase in third-party dependencies

(continued on next page)

for delivering banking products and services, and the repercussions of the COVID-19 pandemic. Operational resilience is defined as both "an outcome that benefits from the effective management of operational risk" and "the ability of a bank to deliver critical operations through disruption" by the BCBS, which defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events." Echoing these views, Acting Comptroller of the Currency Michael J. Hsu recently described operational resilience as "the ability of a bank to prepare for, adapt to, and withstand or recover from disruptions."

Solutions to the challenges of the three-line model have also emerged during this time, alongside a prioritization of first-line defense. The IIA in July 2020 released a much-anticipated update to its 2013 position paper titled "The IIA's Three Lines Model: An Update of the Three Lines of Defense." In addition to dropping "of Defense" from the new "Three Lines Model" (TLM), the update made changes to address the issues of adaptability, proactiveness, collaboration, and efficiency. Among them:

- A more strategic role for risk management;
- Heightened focus on the role of management of the first and second lines;
- More discretion in the design, structure, roles, and responsibilities across those lines; and
- Greater adaptability in accordance with a bank's needs, complexity, size, and readiness.

Shortly thereafter, in March 2021, the BCBS released "Revisions to the Principles for the Sound Management of Operational Risk," an update to its 2011 original release that was also long-awaited following a comprehensive review of effectiveness in 2014. That same month the committee also released its "Principles for Operational Resilience."

The BCBS's revisions to operational risk principles placed a heavy focus on the key responsibilities of "business unit management" (the first line of defense) to accomplish the following:

- Ensure internal control environments are effective;
- Monitor and report on the business unit's risk profile relative to the bank's risk appetite and tolerances;
- Leverage risk identification and assessment tools such as risk and control self-assessments (RCSAs); and
- Employ strong change management practices that enable a more preventative and proactive risk management posture.

The BCBS also highlighted the growing need for first-line accountability for information and communication technology (ICT), business continuity, third-party dependency, cybersecurity, and broader incident and disruption risk management, which is expanded upon in the operational resilience principles.

Solutions to the challenges of the three-line model have emerged alongside a prioritization of first-line defense.

Areas where we've seen banks under tremendous scrutiny include the assessment of overdraft fees, servicing-related disclosures, application of payments, dispute handling, and fee and interest assessments.

As recently as March of this year, Hsu gave a speech at the Institute of International Bankers' annual conference titled "Thoughts on Operational Resilience." Drawing on a paper released by federal financial agencies in October 2020 titled "Sound Practices to Strengthen Operational Resilience," he previewed work the agencies are undertaking to establish "baseline operational resilience requirements for large banks with critical operations"—notably including their third-party providers. We should anticipate requirements such as the following:

- Better identification and risk management of critical activities;
- Definition of tolerances;
- Scenario modeling of specific disruptions;
- Testing of resilience capabilities;
- More stringent requirements and management of third-party providers, particularly critical service providers; and
- Related governance and risk management standards.

In addition to the rapidly increasing expectations of the first line's responsibilities for enterprise-wide risk management, the bank regulators have also shifted much of their supervision and enforcement attention away from the programmatic and governance-related areas of risk management. Their focus has turned toward the operational execution of products and services, related adherence to regulatory compliance requirements, and effectiveness of internal control environments. Areas where we've seen banks under tremendous scrutiny in the past couple of years, and where enforcement actions have abounded, include the operational execution of all requirements related to the Electronic Fund Transfer Act's Regulation E, activities related to the assessment of overdraft fees, servicing-related disclosures, application of payments, dispute handling, and fee and interest assessments.

Notable enforcement actions have included a December 2022 consent order by the Consumer Financial Protection Bureau (CFPB) covering a broad scope of unfair acts and practices across a major bank's auto, mortgage, and deposit account servicing. These included incorrect assessment of fees and interest and application of payments, incorrect denials on mortgage loan modifications, and improper account fee waivers, overdraft fees, and account closures. The CFPB levied a $1.7 billion civil money penalty and required more than $2 billion in consumer redress.

Additionally, two other banks were the subjects of enforcement actions by the CFPB and Office of the Comptroller of the Currency (OCC) in July 2022 and December 2023, respectively, for Reg E-related violations in the management and distribution of prepaid card-based unemployment insurance benefits. For one bank, this culminated in paying $100 million to the CFPB, $125 million to the OCC, and a full redress to impacted customers. The other paid $15 million to the CFPB and OCC and approximately $5.7 million in redress. Separately, another two banks received enforcement actions in June 2023 and September 2022, respectively, related to their overdraft fee-related practices. One was fined $60 million by both

(continued on next page)

the CFPB and OCC, and was required to provide redress of approximately $80.4 million, and the other was fined $50 million by the CFPB and required to provide redress of approximately $141 million.

Mounting Pressure on the First Line

Clearly, the risks are very high and the consequences severe for non-compliance—particularly where it creates consumer-related harm. And none of this is simple. Most, if not all, of these regulations are extensive and complex in their requirements, and very difficult to implement and execute to perfection, particularly as the bank delivery model becomes increasingly dependent on third parties and advanced technologies. The pressure on the first line to effectively anticipate, understand, and manage the expanding scope of risks is intense.

As we see the bar continue to be raised for compliance, consumer protection, and operational risk and resilience, we also see the interpretation of the LOD Model/TLM shifting in tandem. With this change, we have seen a trend in banks building out first-line "risk and control" functions, even going so far as to designate a "Chief Control Officer," with reporting lines to the business instead of the second-line CRO function. The intention of this model is to reinforce and deepen first-line accountability for risk, and there are many examples proving this to be an effective approach. But one can also argue, and there are examples of this as well, that this new model could diminish the significance of the second-line functions and the roles of the CRO and CCO. If so, it could dilute the framework of risk-related "checks and balances" that has been established, create possible conflicts in the interpretation of risk appetite, and introduce role confusion of another kind altogether.

Conclusion

The regulatory pressure on banks has never felt more intense, and the stakes are high. Still, the risk management talent and expertise in the industry has never been stronger. Now, it remains to be seen which designs and interpretations of the LOD model/TLM will be most effective at harnessing that expertise in a manner that enables the proactive, efficient, collaborative, and strategic risk management that is required.

Clearly, the risks are very high and the consequences severe for non-compliance—particularly where it creates consumer-related harm.

Karin Lockovitch

Karin Lockovitch, a Treliant Senior Managing Director, is a 25-year banking and financial services executive. At Treliant, she leads the Regulatory Compliance, Mortgage, and Operations Solutions practice, providing clients with valuable, applicable, and innovative solutions and support for their regulatory and risk management needs.

Laura Huntley

Laura Huntley is a Managing Director in Treliant's Regulatory Compliance, Mortgage, and Operations Solutions practice. Laura brings almost two decades of specialized experience in regulatory strategy, compliance, and risk management within the financial services industry, having worked both as a practicing attorney and a risk and regulatory consultant.
LHuntley@treliant.com

Treliant, an essential partner to financial services companies globally, brings to you *The Pulse*, a quarterly newsletter offering insights and information regarding pertinent issues affecting the industry. This article appeared in its entirety in the Spring 2024 issue. Other articles that appeared in this issue include:

- Operational Risk: A Deciding Factor in Financial Services M&A
- SEC Introduces Climate Disclosure Requirements, Litigation Intensifies
- Bitcoin: Finance on the Modern Frontier

To subscribe to our quarterly newsletter, *The Pulse,* visit **Join Our Newsletter - Treliant.**

Treliant®