

International Journal of **Finance** (IJF)

**Breaking Down Barriers: Adapting Three Lines of Defense for Ever
Changing Banking Regulations**



**CARI
Journals**

Breaking Down Barriers: Adapting Three Lines of Defense for Ever Changing Banking Regulations

 Kinil Doshi

Independent Researcher,

New Jersey, USA

<https://orcid.org/0009-0001-2547-6828>

Accepted: 3rd Mar 2024 Received in Revised Form: 3rd Apr 2024 Published: 3rd May 2024

Abstract

The changing regulatory landscape presents a significant challenge to banks. This paper discusses the challenges associated with adapting the Three Lines of Defense (3LOD) model in order to comply with regulatory changes within the banking industry. The paper focuses on the challenges of adapting to the rapidly evolving banking regulatory environment. The three lines of defense (LoDs) model is a framework that enables banks to manage risk and compliance with regulatory requirements with precision and accountability. The 3LODs are based on a three-line strategy. The LLOD model enables a bank to identify and manage risks accurately and effectively. The use of technology and analytics can enable banks to automate control checks to improve the speed and precision of their control checks. To conclude, banks need to refine the three lines of defense to keep up with an ever-evolving regulatory environment to ensure compliance with rules, identifying risks accurately, and enhancing their risk management capabilities.

Keywords: *Risk Management, Three Lines of Defense (3LOD), Banking Regulations, Control Framework, Risk Mitigation.*

1. Introduction

The changing regulatory landscape presents a significant challenge to banks. A number of banks have also been fined for non-compliance. Here are a few examples that have been reported -

- A \$7.2 billion fine was paid in 2017 by Deutsche Bank in connection with allegations of mis-selling mortgage-backed securities in the United States¹
- In 2018, HSBC agreed to pay \$765 million to settle allegations that it handled residential mortgage-backed securities in a negligent manner.²
- A \$3.9 billion settlement has been reached between Goldman Sachs and the 1MDB scandal, where the bank was accused of laundering billions of dollars.³
- A \$920 million fine as a result of spoofing and manipulating precious metals and Treasury markets was paid by JPMorgan Chase in 2020.⁴
- U.S. regulators fined Citigroup \$400 million in 2020 for "long-standing deficiencies" in its risk management and internal controls.⁵

Therefore, banks must tighten their risk management and adhere to a growing number of regulatory requirements. In order to address the challenges of regulatory compliance and risk management with precision and accountability, the strategic implementation of the Three Lines of Defense (3LOD) model is becoming increasingly important.

This paper discusses the challenges associated with adapting three lines of defense in order to comply with regulatory changes within the banking industry. It emphasizes the Three Lines of Defense framework as a means of enforcing control, managing risk, and ensuring regulatory compliance. Additionally, this paper aims to:

- Examine the complexities of adapting to the rapidly evolving banking regulatory environment.
- Detail the Three Lines of Defense model and its critical role in fostering a culture of compliance and risk awareness.
- Offer actionable insights and strategies for the effective implementation of the 3LOD model.
- Provide guidance for navigating common challenges

The Three Lines of Defense Model:

The Three Lines of Defense model⁶ organizes risk management and control structures within banks, delineating clear responsibilities and accountability across different layers:

First Line of Defense (1LOD) - Business Operations: This layer encompasses banks' operational and business units, responsible for directly managing risks associated with their activities. Their primary tasks include early risk identification, prevention, mitigation, and adherence to regulations and organizational policies.

Second Line of Defense (2LOD) - Independent Compliance and Risk Management: This layer oversees and manages risk in an independent manner from operational management and executive leadership. It is responsible for development of a risk management framework and strategy. 2LOD is also responsible for setting risk appetite, and monitoring risk exposure.

Third Line of Defense (3LOD) - Internal Audit: Internal audit functions as an independent assurance layer. 3LOD evaluates the effectiveness of risk management and compliance practices implemented by the first and second lines of defense.

It is imperative to focus on strategic alignment of 3LODs along with technological advancement in order to address to regulatory compliance as well as bank's stability.

2. Grasping the Three Lines of Defense Model

To ensure fiscal stability and adherence to regulations, a solid control system is imperative in the management of banking risks. This purpose is well served by the Three Lines of Defense (3LOD) model⁷ by segregating duties among different units within a financial institution.

1. First Line of Defense (1LOD) - "Front-line/Business"⁹

This is the first protective layer, commonly called the "front-line" or "business." It includes operational staff, business heads, and employees involved in risk-generating work. The obligation to effectively assess, manage, and reduce risks associated with their roles falls on them. By promoting proactive risk detection & mitigation, the first line of defense cultivates a working atmosphere where risk awareness and ownership are encouraged.

Primary duties of the First Line of Defense include:

- Conducting thorough risk analyses in order to identify potential threats and weaknesses.
- Implementing strong control measures to reduce known risks.
- Regularly monitoring and mitigating risks
- Partnering with the second line of defense to ensure appropriate risk management.
- A strong first line of defense plays an important role in managing risk, creating a strong risk culture, and aligning risk taking with organizational goals.

2. Second Line of Defense (2LOD) - "Independent Compliance and Risk Management"

The second line of defense plays a major role in keeping an eye on things. They set the firm's Risk & Compliance Framework. They monitor and evaluate the effectiveness of the first line's internal controls and reporting any suspicious activity. Identifying risks and implementing mitigation strategies are their responsibilities. They also respond to audits and regulators.

Primary duties of the Second Line of Defense entail:

- Establish a risk management framework tailored to the firm's size and complexity, and meets all rules and regulations.

- Provides advice and support to the first line in understanding and managing risks.
- Assumes responsibility for assessing and reducing risk independently.
- Ensuring adherence to regulations and internal policies
- Collaboration with Senior Leadership, the first line of defense, and Internal Audit to ensure that risks are appropriately managed.

3. Third Line of Defense (3LOD) - "Internal Audit"

An internal audit serves as a third line of defense by evaluating and improving the risk and control effectiveness.

Primary duties of the Third Line of Defense line include:

- Ensure compliance, independently oversee risks, and reinforce internal controls.
- Assist the Management and Board Risk Committees with independent and objective assurance
- Provides advice and support to the first line in understanding and managing risks.

3. Role of the First Line of Defense (1LOD)

Business Units are primarily responsible for managing the risks. They identify, understand, and deal and mitigate risks. 1LOD's responsibilities are described below.¹⁴

Risk Assessment: The first step in assessing risks is to identify the risk. It is important for 1LOD to understand their own business risks. There are several types of risks that may occur. They may be classified as credit, market, liquidity, regulatory, compliance, operational, financial and other non-financial risks. Identifying and monitoring these potential risks early can assist in preventing or reducing them in the future.

Establishing controls: Once the risks are identified, the first line enforces controls to deal with them. To ensure compliance with regulations, they implement strong processes and controls. Additionally, they monitor the effectiveness of these controls and make any necessary adjustments.

Compliance with regulations: Following all regulations is an essential part of the banking industry. Business functions have a crucial role to play. They ensure that their teams adhere to the rules & regulations. This means they must understand the new regulations and put safeguards in place. They need to keep up with changes, check for risks, and control threats related to non-compliance.

Developing a culture of risk awareness: 1LOD are responsible for fostering a culture of risk awareness. Their role is to create an environment where risk awareness is an integral part of the daily routine. It is everyone's responsibility to control risks. Continuous training and education are essential. It is crucial to be aware of risks and to prevent them in advance. 1LOD is responsible for preventing risk within a financial institution. They manage risk linked to their actions, put

procedures & controls in place, ensure regulatory compliance, and promote risk awareness. In doing these things well, 1LOD supports the bank's overall stability

4. Role of the Second Line of Defense (2LOD)

Banks's second line of defense is independent compliance and risk management. They are responsible for monitoring the bank's risk management practices. It is an independent function. There is no interference from the CEO or the front-line personnel in their work. 2LOD's responsibilities are described below.

Managing risks: ¹⁰ 2LOD is responsible for assessing and balancing risks. 2LOD monitors all risks. In order to mitigate risk, they identify possible non-compliance areas and work with business functions to develop corrective action plans.

Establishing a Risk Framework: The second line of defense is responsible for establishing a risk framework. It must be in accordance with the bank's profile. They develop policies, procedures, and directives. This uniform risk management approach strengthens the bank's processes and controls. It enables them to navigate the volatile financial market.

Standalone Assessment: Standalone evaluation is an important aspect of the second line of defense. The unit functions independently of the front-line units. By doing so, it is able to give an unbiased assessment of the bank's risk situation. Risk management practices are regularly reviewed to ensure their effectiveness. Additionally, they ensure regulations are followed and identify opportunities for improvement. The Second LOD, is essential to avoiding financial difficulties. Checks and reduces hazards, establishes a comprehensive safety model, and provides a comprehensive risk appetite for the organization. Performing these duties enhances the bank's overall risk handling capabilities.

5. Role of the Third Line of Defense (3LOD) ¹⁴

Third Level of Backup (3LOD), or Internal Audit, is an important component of the bank's safety framework for ensuring that all steps, rules, and processes are followed. The purpose of internal auditing is to maintain effective safety controls and ensure compliance with rules within a financial institution. Their responsibilities include

Compliance and Assurance Review: The main purpose of the 3LOD is to ensure that the bank follows its own rules and regulations. They examine different parts of the bank, such as the front-line units (1LOD) and independent risk groups (2LOD). The focus is primarily on what has been done to minimize risks associated with finance, credit, markets, liquidity, and other non-financial elements. By conducting thorough checks, the 3LOD provides the board audit committee and senior management with a reliable analysis.

Independently Assessing Risk: The 3LOD is responsible for checking that rules are being followed as well as monitoring risk-taking. In its role as a separate entity, the 3LOD is able to observe and evaluate risks and how they are handled without any bias. By identifying risks early,

monitoring and managing them efficiently, they ensure bank's financially stable. Additionally, they assist the bank in adjusting to new regulatory requirements as they arise.

Strengthening internal controls: Internal detects any gaps or weaknesses in the controls set by the 1LOD and 2LOD by testing the effectiveness of the controls. This provides the bank's management with a clearer understanding of where improvements are needed in risk management. The 3LOD plays an important role in ensuring that a bank complies with all regulatory requirements and follows the best standards.

Strengthening Business Continuity Risk Management: The 3LOD's role is to inspect business continuity risks. It assesses how well the organization is prepared to handle disruptions. The 3LOD assists in the development of strong business continuity plans.

In ensuring compliance with regulations and maintaining effective risk control, the third line of defense (3LOD), or Internal Audit, plays an important role. During this process, IA assess compliance, review risks independently, improve internal controls, and ensure robust business continuity planning. The 3LOD provides valuable insight to senior management on risk management and regulatory compliance through comprehensive audits and evaluations.

6. Strengthening the Three Lines of Defense Model for Regulatory Changes¹⁰

Regulations in the banking industry are constantly evolving. A strong risk management culture must be promoted by financial institutions through the continual updating of their control frameworks. The Three Lines of Defense (3LOD) aids in managing risks and regulatory compliance framework. To improve the 3LOD model in order to address the challenges introduced by changing regulations, the following factors must be taken into account.

Reforming the operating model: As a result of changing regulations, financial institutions must be more agile in adapting their operating models to become more global in nature. It is imperative that talent models be improved, skill shortages be identified, and resources be aligned to handle new regulatory issues. Moreover, organizations must rethink their location strategies for access to key markets and regulatory authorities.

Streamlining the framework: Banks need to ensure that controls are layered across departments so that compliance with regulations can be easier. In other words, a one-size-fits-all list of control steps and tasks is necessary to meet regulatory requirements. A change in testing method can help banks become more efficient, faster, and provide better results in assessing the effectiveness of their control systems.

Developing technology-enabled internal control functions: In today's digital age, banks can leverage new technology solutions, artificial intelligence models, and big data analysis to enhance their internal control functions. Control testing can be automated to save time and resources. It also helps spot possible compliance issues. Analysis of big data can provide useful information by identifying patterns that indicate non-compliance or new risks. In most financial institutions, technology enablement has resulted in significant improvements in internal control functions. New

technologies, such as AI, ML, and robotic process automation, have improved efficiency and reduced operational risks.

Banks should smartly change their working models, merge control frameworks, and use technological solutions to improve the Three Lines of Defense model. This will enhance risk management, improve regulatory compliance, and allow banks to adapt to ever-changing regulations.

7. Enhancing Operation Modes for Better Risk Management

Management of risk and compliance with regulatory requirements are essential in the rapidly evolving banking industry. In order to meet the risks associated with a fluid regulatory environment, banks must adapt their ways of operating. They can utilize the Three Lines of Defense (3LOD) strategy. 3LOD are, namely a first line, a second line, and a third line of defense. However, in order to effectively manage risks, banks must consider reshaping their operations, rationalizing their strategies, and utilizing technology. A bank's operating system must be overhauled in order to become more effective worldwide. It is imperative that they reconsider their structure, processes, and decision-making processes. By implementing these changes, banks will be able to develop a mode of operation that is capable of effectively managing risks and adapting to regulatory changes. There may be a need to reshape talent systems, plan locations, and make better use of resources as a result of these changes.

Another vital part of risk management is strategy rationalization. As a result, controls must be uniform throughout the bank and testing procedures must be simplified. This allows banks to expand, streamline, and improve their control systems. This ensures that all parts of the bank are closely monitored and checked for compliance with risk and regulatory requirements. Modern risk management heavily relies on technology innovation. Banks can transform their internal control functions into digital ones using the latest technology, artificial intelligence and smart analytics. It facilitates automation, better data analysis, and real-time risk monitoring. Using technology can benefit banks in ensuring compliance with rules, identifying risks accurately, and enhancing their risk management capabilities.

In order to effectively manage bank risk, it is crucial to redesign operation models, rationalize frameworks, and implement enabling technology. Banks can handle regulatory shifts, spot risks early, comply with rules, and maintain financial health by optimizing operating structures, matching control frameworks, and using tech solutions.

8. Rework of the framework for matching controls

The dynamic nature of the banking industry requires robust risk management. In this regard, framework rationalization becomes important. It facilitates the coordination of risk controls and improves the testing process. As a result, banks will be able to comply with regulations and remain financially secure.⁸⁹

What is the importance of framework rationalization?

Every bank needs a strong risk management framework in order to reduce financial market dangers. Framework rationalization helps reach this goal by simplifying controls and removing duplicate efforts. It provides consistency in meeting regulatory requirements and applying best practices throughout a banking organization.

The Benefits of Framework Rationalization

Better Risk Spotting: By implementing a rationalized risk management system, bank can gain a comprehensive understanding of its risk exposure. Early risk detection and evaluation result in speedy risk reduction methods and informed decisions.

Simplified Tasks: The alignment of control and testing duties eliminates needless repetition and reduces compliance workload. As a result, operational effectiveness is enhanced. By doing so, the risk management team will be able to focus on more pressing issues.

Expanded Coverage: Making sense of the framework allows all significant risks to be addressed in the appropriate manner. By linking controls to specific risks, banks can increase risk coverage and limit overlooks.

Financial institutions can streamline controls in their framework by following the following tips:

Comprehensive Evaluation: There is a need to conduct a meticulous review of current controls, systems, and frameworks across a range of defense lines. Identify overlaps, imperfections, and areas that need to be aligned.

Control Mapping: Controls should be assigned in accordance with specific risks and regulatory requirements. Having these controls in place ensures that every risk is sufficiently addressed.

Revamping Testing Protocol: Ensure that the testing is aligned with the aligned controls. The redesign of test methods should focus on the primary areas and emerging risks in order to increase coverage and effectiveness.

Training and Messaging: Everyone involved, such as business units on the front line, risk management groups, and internal auditors, should be trained and provided with clear communication.

9. Using Tech to Upgrade Internal Control Operations

Tech advancements have led to significant changes in banking operations, including internal control. Banks are using more technology to manage risks as banking rules are constantly changing.

12

Redesigning the way they operate: Globally, banks are remodeling their operations. New technology is causing them to rethink their teams and where they work. Banking operations can be improved and made more efficient with the use of digital tools and automated processes.

Streamlining the testing and control processes: Managing risks in the banking industry requires streamlined controls. Banks are integrating and standardizing controls across their business in order

to avoid repeating actions and to ensure consistency. A major component of this process streamlining is the redoing of the testing process. In order to ensure compliance with regulations, banks need to take a focused approach to testing.

Harnessing New Tech and Advanced Analysis: Digital banking upgrades rely heavily on technology. New technologies and detailed analytics are being used to manage and mitigate risk. Artificial intelligence (AI), machine learning, and robotic process automation (RPA) are used in routine tasks and unravel complex data. Technology allows banks to identify risks early, to make smarter decisions, and to utilize resources more efficiently.

The financial sector is turning to technology to cope with changing regulations. It is reshaping its operations, combining controls, and using new technology tools to do so. The shift to digital and automated systems helps banks manage risk more effectively, work more efficiently, and meet regulatory requirements.

10. Dealing with Regulatory Changes

It is crucial to manage regulatory changes in the banking sector in order to manage risk. Due to the dynamic regulatory landscape, banks must regularly update their procedures, rules, and checks. They utilize new technology tools, revamp test processes, and blend controls in order to adapt.

Simplifying Controls: The importance of ensuring consistent, efficient risk management across the bank cannot be overstated. A simplified control structure can streamline testing, broaden coverage, and enhance control effectiveness. This process involves reviewing current controls, eliminating duplicate efforts, and aligning controls with regulatory requirements.

Leveraging Technology: Keeping pace with regulatory changes requires updating internal control systems with digital technologies. The use of new technology and analytics can enable banks to automate control checks in order to improve the speed and precision of their control checks. As a result, risk management teams are able to spot and resolve potential compliance issues, thereby reducing the risk of rule violations.

Revamping the Operating Model: Operating models should be swift and efficient in the fast-paced world of banking. Risk management can be improved by making adjustments to operating structures, employee models, and office location strategies. It entails reevaluating the duties and roles within the framework of the three lines of defense. It involves clear roles and smooth teamwork between frontline businesses, independent risk management, and internal audit.

Conclusion

This paper covered the importance and effectiveness of the Three Lines of Defense (3LOD) model in enhancing the regulatory compliance and risk management capabilities within the banking sector. By detailing the distinct roles and responsibilities of each line of defense it underscored how this structured approach can significantly improve a bank's ability to manage risks and comply with increasingly complex regulatory demands.

Through the strategic implementation and continuous refinement of the 3LOD model, banks can achieve a robust governance framework that not only meets current regulatory requirements but also adapts to new challenges as they arise. Banks can enhance their risk management processes and maintain financial stability by integrating advanced technological solutions and optimizing operational models.

In conclusion, this study confirmed that the Three Lines of Defense model is not only beneficial but also essential for banks to navigate the landscape of banking regulations. The model has proven effective in fostering a culture of compliance and risk awareness that aligns with organizational goals.

Recommendation

For banks to effectively implement this blueprint, they should consider upgrading their operating models, refining their framework, and exploiting technology. It is necessary to revamp operating systems in order to facilitate swift, efficient global operations. Streamlining controls and reshaping test processes increases coverage, efficiency, and effectiveness. It is also important to invest in technology solutions and advanced analytics.

References

¹[https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-72-billion-misleading-investors-its-sale-residential-mortgage-backed#:~:text=The%20Justice%20Department%2C%20along%20with,RMBS\)%20between%202006%20and%202007](https://www.justice.gov/opa/pr/deutsche-bank-agrees-pay-72-billion-misleading-investors-its-sale-residential-mortgage-backed#:~:text=The%20Justice%20Department%2C%20along%20with,RMBS)%20between%202006%20and%202007)

²<https://www.reuters.com/article/idUSKCN1MJ23W/>

³<https://www.reuters.com/markets/asia/goldman-sachs-its-role-multi-billion-dollar-1mdb-scandal-2023-10-12/>

⁴[https://www.reuters.com/article/idUSKBN26K321/#:~:text=\(Reuters\)%20%2D%20JPMorgan%20Chase%20%26,U.S.%20authorities%20said%20on%20Tuesday.](https://www.reuters.com/article/idUSKBN26K321/#:~:text=(Reuters)%20%2D%20JPMorgan%20Chase%20%26,U.S.%20authorities%20said%20on%20Tuesday.)

⁵<https://www.complianceweek.com/regulatory-enforcement/citigroup-fined-400m-for-compliance-risk-management-failures/29588.article>

⁶ A Guide to the 3 Lines of Defense in Compliance

⁷ Understanding Three Lines of Defense in financial services | the fundamentals

⁸ IMF - Regulatory Reform 10 Years after the Global Financial Crisis

⁹ OCC Guidelines Establishing Heightened Standards

¹⁰ Deloitte - Modernizing the three lines of defense model.

¹¹ Three Lines of Defense: A New Principles-Based Approach

¹² Financial Stability Board (FSB) - "Principles for Effective Risk Data Aggregation and Risk Reporting"

¹⁴ The Three Lines of Defense (LOD) in Security and Compliance: Roles, Challenges, and Tools

¹⁵ Adapting Three Lines of Defense (LoD) to navigate through ever-changing Banking Regulations

¹⁶ How to Apply the Three Lines of Defense



©2023 by the Authors. This Article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>)