



LESSONS LEARNED

Risk Management and the Three Lines Model

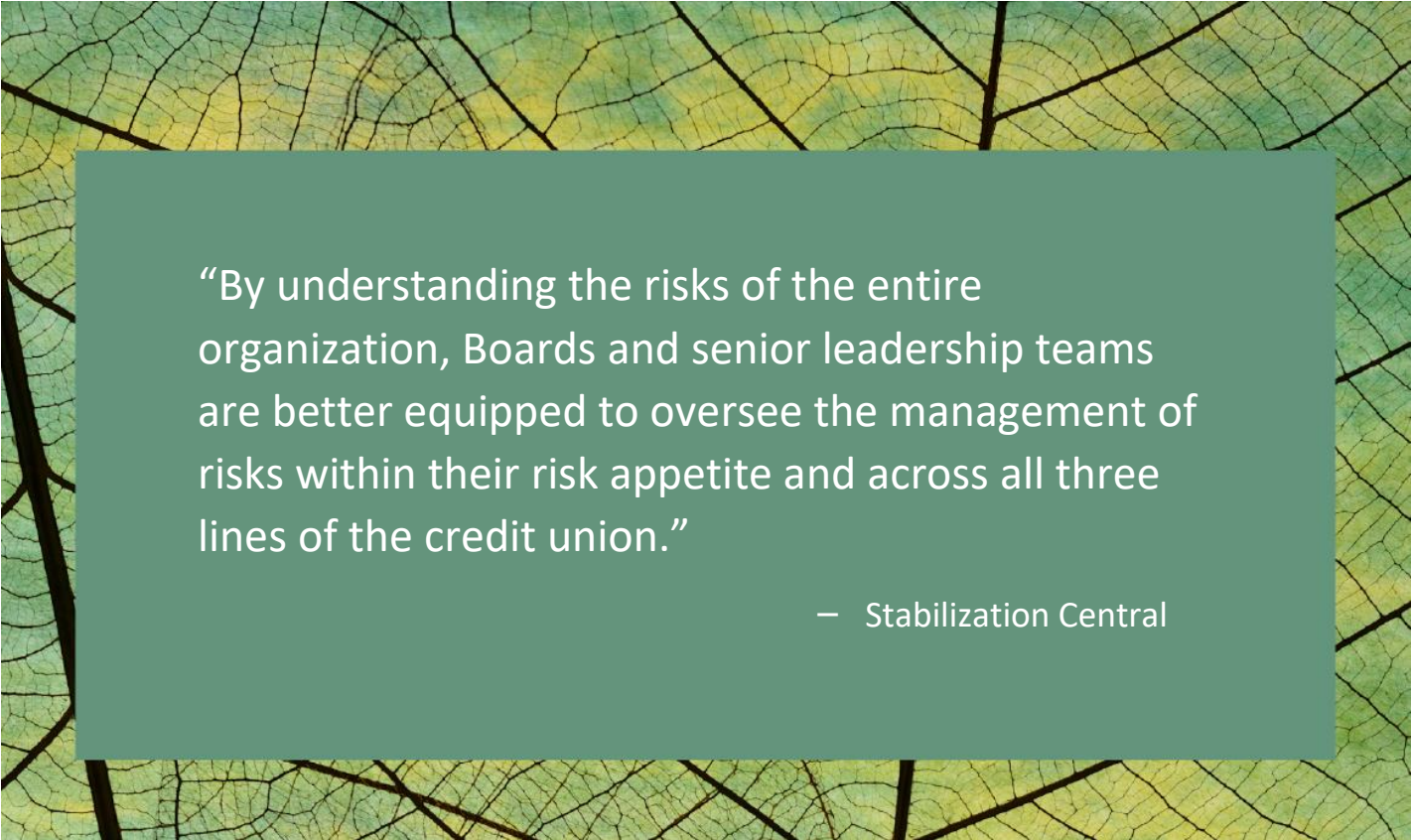
Prepared by: Bill Corbett, Frank Chong, and Mary Falconer.

December 2022

Stabilization Central
— CREDIT UNION —

Table of Contents

Background	3
Enterprise Risk Management Framework and Internal Control	3
Regulatory Expectations	4
Three Lines Model	4
First Line	4
Second Line	5
Third Line	5
Responsibilities of the Board and Senior Management	6
External Assurance Providers	6
Additional Tips	7
Copyright and Disclaimer	8



“By understanding the risks of the entire organization, Boards and senior leadership teams are better equipped to oversee the management of risks within their risk appetite and across all three lines of the credit union.”

— Stabilization Central

Background

Stabilization Central Credit Union (“Stabilization Central”) is committed to the stability and strength of the credit union system and is uniquely positioned to assist with navigating continuously changing risk environments and regulatory requirements. Credit unions face a myriad of risks in their day-to-day operations, and each credit union makes decisions on how to utilize organizational structure, policies, and practices to manage these risks. Senior management and the Board of Directors (“Board”) will need to consider the strategy, size, and risk appetite of their credit union to ensure adequate measures are in place to protect the members and the business in both strong and challenging economic times.

This paper within the Lessons Learned series explores the importance of risk management and the Three Lines Model (formerly referred to as Three Lines of Defence but recently updated by the Institute of Internal Auditors). It provides an overview of Board and senior management roles and responsibilities as well as risk management best practices, and it outlines current regulatory expectations. We also highlight the importance of evolving a credit union’s risk management practices as it grows and becomes more complex, including through continuous reviews and reassessments. The aim of this paper is to offer credit unions guidance and explain how they can enhance their risk management practices by utilizing the Three Lines Model.

Enterprise Risk Management Framework and Internal Control

Financial institutions are in the business of taking risks, including credit, market, liquidity, capital, and operational risks, to name a few. Since the financial crisis in 2008, regulatory expectations surrounding internal controls and enterprise risk management (“ERM”) have continued to increase in complexity to protect the stability of the financial system and to prioritize financial and operational resilience, especially in light of the ever-changing economic environment and the continuing impacts of the pandemic, geopolitical tensions, supply-chain

challenges, and government monetary policy to manage inflationary pressures.

In addition to maintaining regulatory compliance, credit unions must ensure that they are adequately managing the risks in their operations and that their internal control structures support the management of risks inherent in their strategy and business models.

These are some key areas for credit unions to consider:

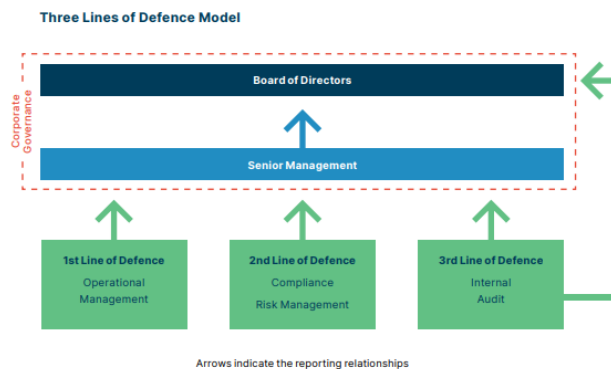
- The Board must understand the expectations placed on each board member within the legislative and regulatory framework with respect to risk management. This includes ensuring that the credit union’s business model risks are well understood and that corporate governance structures and practices are in place to assist the Board in overseeing and monitoring those risks.
- Management must establish a strong internal control environment by creating appropriate policies, procedures, and systems and employing competent and skilled personnel.
- The ERM framework (including risk appetite) and internal controls must be evaluated against changing business and operational environments — especially as credit unions evolve, grow, and become more complex. Mechanisms must be in place in the corporate governance structure to ensure continuous monitoring is occurring.

Appropriate risk management sets a strong foundation and ensures that credit unions can identify, assess, and respond proactively to risks within their business operations. It also provides a mechanism to reduce the likelihood that a risk will have negative impacts. All employees of a credit union have a responsibility to effectively manage risk.

Regulatory Expectations

Regulators¹ must balance the safeguarding of depositor and stakeholder interests and the need for prudent regulation (including comparability to federal and international regulatory standards) against the realities of the local market environment and the ability for provincially regulated financial institutions (“PRFIs”) to remain competitive and take reasonable risks. Regulators take a principles-based approach, utilizing risk-based supervision to assess whether the risks a PRFI takes are appropriately managed. Accordingly, regulators generally scale regulatory expectations to all credit unions, based on differences in size, complexity, and business models.

In their supervisory framework, regulators provide guidance on their approach to credit union risk assessment, including an overview of the methodology used in assessing the quality of risk management. Included in Appendix B of the supervisory framework is the characterization of a credit union’s risk management under a “Three Lines Model,” as shown below:



Source: BC Financial Services Authority (BCFSA), [Supervisory Framework for Provincially Regulated Financial Institutions](#) (September 2021).

In the next section, we will examine this model in more detail and provide a practical approach to

organizing your risk management function utilizing this model.

Three Lines Model

In 2013, the Institute of Internal Auditors developed the Three Lines of Defence Model (now the Three Lines Model), and it has become the most common approach to assigning control and risk management responsibilities within organizations. As outlined above, it is common for regulators to utilize this model in their supervisory approach. Essentially, this model is characterized by three main principles:

(Source: Oliver Wyman Analysis).

- 1) Accountability — ensuring that those parts of the credit union taking the risks are accountable for those risks.
- 2) Independent challenge — creating an independent control function to ensure risks are identified, assessed, controlled, and managed within appropriate risk tolerances and metrics.
- 3) Independent assurance — establishing a regular assurance process that assesses the interactions between those accountable for risk and the independent control function and reporting those assessments to the appropriate corporate governance oversight functions.

How credit unions incorporate the three lines into their organizational structure will depend on their business model, associated complexity, and risk profile. The following is a brief overview of each line:

First Line

Typically, the first line is comprised of the business units — those that control and manage the day-to-day operations of the credit union. The model assigns the basic risk management and control responsibilities to the first line, which ensures a balance between generating business for the organization and remaining conscious of the

risks and control procedures. The first line must have a clear understanding of the credit union's ERM framework and its risk appetite in order to fully manage their responsibilities in keeping with the desired risk and control environment.

Second Line

The second line is independent of the first line and is comprised of various risk management and compliance functions (i.e., support functions) that monitor and report on all types of compliance, risk, and financial control issues. The second line:

- Guides the creation of the ERM framework and the risk appetite statement, assisting the Board with creating the right balance of business growth/strategy and risk for the credit union.
- Ensures that preventive and detective control requirements are included in the procedures and policies of the first line.
- Applies defined risk-assessment criteria and utilizes controls on an ongoing or periodic basis.
- Oversees the risk identification process (including external and emerging risks) and reports to senior management and the Board (bottom-up capture).
- Ensures that an effective feedback loop occurs via regular Board and senior management risk discussions at the strategic level, and yields outcomes that result in appropriate risk parameters and indicators (top-down capture).

In smaller, simpler credit unions, these functions could reside with a role combining responsibilities of the chief financial officer ("CFO") and the chief risk officer ("CRO").

Third Line

The third line is comprised of the internal audit function. For this function to be effective, it must have the highest level of objectivity and independence. Internal audit must:

- Conduct, at a minimum on an annual basis, a risk assessment of the organization and incorporate this into creating a risk-based internal audit plan.
- Assess the credit union's ERM framework and risk appetite as key components of the internal audit plan, as they provide a foundation for evaluating the credit union's risk and control environment and guiding the urgency and materiality level of any findings.
- Provide both senior management and the Board with assurance on a range of items — including efficiency and effectiveness of operations, compliance with laws and the regulatory framework, safeguarding of assets, and integrity of reporting processes. At times, the internal audit group will also act as an advisor or provide consulting services to support the organization in improving its control and risk processes.
- Have direct access to the Board and report the results of its internal audit activities to them (usually through the audit committee) on a quarterly basis. Functionally, the internal audit group reports directly to the audit committee.
- Take responsibility for ensuring that the relationship between the first and second lines is appropriately close without compromising independence.

Credit unions may utilize external providers to provide some of the second- and third-line functions, depending on the size and complexity of credit union operations. In these situations, it is extremely important for senior management to understand that they still are accountable for the risk, and to ensure they are aware of their responsibilities under outsourcing arrangements, which include:

(Refer to Outsourcing Guideline, issued by BCFA October 2021).

- Ensuring appropriate skill and competency exist in the outsourcing partner relationship.
- Ensuring appropriate risk policies are understood and complied with by the outsourcing partner.

- Managing, overseeing, and evaluating the outsourcing partner’s work on an ongoing basis.
- Appropriately allocating resources to ensure that third-party arrangements are adequately funded and able to provide the appropriate assessment of controls and assurance required by the organization.

Responsibilities of the Board and Senior Management

In order for the Three Lines Model to work successfully, an appropriate level of corporate governance by both the Board and senior management must exist to ensure that each line is operating as intended.

The Board of a credit union, as elected by its members, has a fiduciary responsibility to oversee the credit union’s operations by acting as a steward of the organization and reporting back to the members on at least an annual basis. The Three Lines Model requires the Board to play a critical role in corporate governance. More specific responsibilities include:

- Providing appropriate guidance, review, and approval during the development of the credit union’s strategy, business model, and objectives/plans.
- Ensuring that the appropriate level of competence and skill exist at the senior management level, while also ensuring that compensation models are aligned with the credit union’s best interests.
- Participating in the development of the ERM framework for the credit union. This includes participation in creating key risk indicators and tolerance levels, reviewing and monitoring current risk registers and emerging risks, and assessing new strategies and objectives against the ERM framework and the established risk appetite.
- Establishing, with senior management, the overall risk appetite and associated risk policies. Ensuring, based on these policies, that risk tolerances are adhered to and that emerging risks are managed.
- Establishing direct relationships with and oversight of the second and third

lines of defense. In larger credit unions, this is done through the audit and risk committees of the Board and ensures that the CFO and CRO have direct, independent access to these committees. This includes:

- Fully understanding and approving the annual internal audit plan, which should be seen as a “tool” to provide the Board with insights into the effectiveness of the internal control environment of the credit union they govern.
- Ensuring that all outstanding audit findings are monitored, resolved, and effectively implemented and are sustained in the internal control framework on a go-forward basis.

Senior management manage and oversee the day-to-day operations of the credit union and are responsible for:

- Developing (for Board approval) the business model, strategic plan, goals, and objectives, included related risks, and ensuring appropriate organizational structure, staffing, and operational policies/procedures are in place to execute those plans.
- Establishing the appropriate corporate and risk culture within the credit union and ensuring strong corporate governance practices exist.
- Maintaining strong communication with the Board and reporting frequently on progress against established financial, risk, and performance metrics.
- Ensuring appropriate and timely resolution of control or risk issues/deficiencies raised and remaining committed to improvements in risk management practices and control structures.

External Assurance Providers

There are also additional external parties that supplement the above Three Lines and assess

the overall risk and control environment of credit unions. As regulated entities, credit unions are subject to supervisory reviews by regulators and must also have their financial statements audited by external auditors on an annual basis. External auditors and regulators are an important part of the overall governance and control structure, as they must abide by professional standards and are ultimately responsible for assessing whether credit unions are adequately complying with regulatory and financial standards and rules.

Although external assurance providers offer an additional form of comfort, credit unions should strive to achieve a strong control and risk environment, the ultimate objective being that no problematic findings emerge from these assessments. Admittedly, supervisory reviews do normally result in some recommendations, but credit unions should understand and abide by the regulatory framework and minimize any mandatory requirements coming out of these reviews.

Additional Tips

- Maintaining open and honest communication with regulators as well as external and internal auditors about their expectations will ultimately assist credit unions in developing the right risk management structure for their organization's size, complexity, and business model.
- Establishing achievable timelines, objectives, and plans to enhance risk management structures and practices is important. Credit unions need time to evolve and achieve the right balance between cost, efficiency, and prudent risk management.
- The credit union sector is a collaborative environment where peer credit unions are willing to share their experiences and support others. Reaching out to others for support will help credit unions navigate risk practices more effectively and efficiently.
- The risk environment continues to grow in complexity, and embracing best practices and innovative solutions will help credit unions effectively manage their risks.

For more information on how Stabilization Central can assist your credit union with risk management practices and the Three Lines Model, please contact info@stabilizationcentral.com.

Copyright and Disclaimer

Except as expressly permitted in this publication, or by the provisions of the Copyright Act, no part of this publication may be reproduced in any form by any means without the written permission of Stabilization Central Credit Union.

Stabilization Central is not responsible for any errors or omissions contained in this publication and expressly disclaims liability, whether under contract or in negligence or otherwise, to any user, including subscribers and other persons who may use this publication and to members, clients, and customers of such subscribers and other persons.

Stabilization Central expressly disclaims liability for loss or damage, whether direct or indirect, resulting from any use of this publication, including, without limitation, any loss or damage arising as a result of the procedures or forms contained in this publication being determined not to be valid or enforceable or not attaining the end desired by the user.

Stabilization Central

— CREDIT UNION —