WHITE PAPER

RISK CULTURE: A FOUNDATION FOR EFFECTIVE ENTERPRISE RISK MANAGEMENT

Stabilization Central
CREDIT UNION

Table of Contents

1. Introduction 3
2. Risk Culture – the Foundation of an Effective Enterprise Risk Management Program 3
3. Risk Culture – a Competitive Differentiator for Credit Unions..4
4. A Strong Risk Culture is Good for Business 4
5. Risk Culture – An Asset to Tackle Current Headwinds 4
6. Implementing Risk Culture as the Foundation of ERM 5
7. Conclusion 8
8. Appendix A 10

Introduction

Stabilization Central Credit Union ("STAB Central") is dedicated to supporting the resilience of the credit union system through proactively strengthening financial and risk management practices for our members.

Recent events within the Canadian financial sector have once again taught our industry the criticality of embedding a culture dedicated to managing risk. These events make clear that complacency about practice and process has significant consequences, not just for financial outcomes but for reputation. Therefore, a culture deeply rooted in managing risk is the very foundation of good business practice.

This paper provides credit unions' management and boards of directors with an overview of how a strong risk culture is the cornerstone of an effective enterprise risk management (ERM) program. We will highlight how the elements of an ERM framework are interconnected and how risk culture is key to achieving the medium- and long-term strategic goals and objectives of an organization.

> "A strong risk culture gives credit unions the power to effectively achieve their strategies. At times, slowing down, like using brakes on a car, actually allows us to move faster and more safely through a corner."
>
> Bill Corbett, CEO
> Stabilization Central

Stabilization Central is a system partner with the depth of skill and expertise to effectively and efficiently support credit unions in strengthening their risk culture. Credit unions' investment in evolving their enterprise risk management framework goes hand in hand with the need to meet rising provincial and federal regulatory expectations for our members.

Our advisory support services include:

- providing training for boards and management to foster a risk management culture
- reviewing and providing insights into the development of board- and management-level ERM reporting that is forward looking
- assisting boards with viewing risk to strategic objectives holistically
- facilitating the adoption of enhanced oversight of nonfinancial risks, which ultimately have a financial impact upon the organization; these risks include third-party/supplier risk management, cybersecurity, and climatic events.

Risk Culture – the Foundation of an Effective Enterprise Risk Management Program

Having a risk culture does not mean an organization takes no risks. On the contrary, it creates business practices that are followed even when no one is looking. Risk culture describes the norms, values, beliefs, knowledge, attitudes, and behaviours about risk that are shared within an organization. Risk culture, or the absence thereof, plays a significant role in how employees at all levels approach risk taking, decision making, and their own behaviour and conduct. Process does not necessarily guarantee or equate to good business practice, so it is important to ensure a culture dedicated to managing risk is understood as the key pillar supporting a long-term sustainable business.

Organizations with a deeply embedded and positive risk culture have a shared vision and understand how to manage their risk-taking activities for optimal benefit while staying within their governance, risk, and compliance requirements. In essence, a risk culture forms the foundation for effective risk management by influencing how risks are identified, assessed, and managed. Cultivating a strong risk culture creates a strategic advantage for credit unions that can enhance long-term resilience in the face of economic volatility, shifting demographic preferences, revenue challenges stemming from limited market share growth, and competitive pressures.

Risk culture comprises many elements that are qualitative in nature and not readily observable and measurable. However, a heat map like the table below highlights the elements of a strong risk culture that can be observed or evidenced by ways of understanding risk against a credit union's risk appetite.

Risk Culture – a Competitive Differentiator for Credit Unions

Risk is necessary to achieve goals. Understanding risks and their potential severity is critical.

A focus on risk culture can serve as a strategic differentiator between credit unions in several ways.

First, **risk culture shapes decision making**. A strong risk culture incorporates a unified risk awareness into day-to-day decisions at all levels of the credit union. When management and employees share a commitment to understanding and managing risk, they are likely to make decisions that align with the organization's risk appetite and long-term objectives — decisions such as when to take a risk, how to take on a risk, and when not to take on a risk.

Second, **risk culture promotes accountability, ownership, and transparency**. A strong risk culture encourages employees to feel empowered to "speak up" and raise concerns about potential risks without fear of retribution. This sense of ownership and open communication allows credit unions to identify and mitigate risks before they escalate into more serious financial concerns.

Third, a strong **risk culture helps mitigate emerging risks.** Emerging risks such as cybersecurity breaches, climate-related financial risks, and non-compliance challenges (including employee misconduct) require proactive identification and management. Again, a risk culture that rewards speaking up and raising concerns will encourage employees at all levels to be solution focused and address emerging risks in a timely and coordinated manner.

A Strong Risk Culture is Good for Business

A strong risk culture leads to more consistent, aligned, and robust risk management practices, which help credit unions maintain financial stability, even during times of market stress and economic uncertainty. This level of resilience and coordination better supports the efficient allocation of capital, helps manage earnings volatility, and safeguards against overexposure to high-risk activities that can erode financial strength.

Members trust credit unions to maintain their reputations and be safe and reliable financial institutions. A strong risk culture helps a credit union minimize the likelihood of major disruptions, such as fraud, data and privacy breaches, or other adverse events that may erode its reputation and trust.

A strong risk culture maintains a healthy balance between growth initiatives and risk management. It helps safeguard credit unions from engaging in unsustainable growth strategies. It ensures that product innovation, revenue growth, and lending are conducted in a way that aligns well with its risk profile.

Operational efficiency and cost reductions are achievable with a strong risk culture. By identifying inefficiencies and operational risks early and implementing corrective actions, costs related to fraud, operational failures, or fines can be avoided, thereby reducing income loss. These costs can otherwise be substantial and, in turn, significantly damage the credit union's reputation, further eroding income.

Risk Culture – An Asset to Tackle Current Headwinds

1. Margin challenges

By prioritizing a strong risk culture, credit unions may be able to better withstand the current headwinds affecting earnings and capital. With interest rate volatility and competitive pressures, credit unions are facing narrowing margins and earnings compression. A robust risk culture encourages risk taking toward long-term earnings performance by being mindful of not engaging in high-risk

activities beyond the approved risk appetite. Credit unions need to ensure that risk taking is managed in a manner that does not erode capital. A strong risk culture enables better capital management by adopting a more structured decision-making process when considering exposure to high-risk assets and loans.

2. Membership growth

In an environment challenged by limited growth in membership, credit unions need to maintain the trust and loyalty of their existing members while taking steps to attract the next generation of members. A strong risk culture that protects members' data can enhance member confidence, especially given the growing demographic favouring digital platforms.

3. Cybersecurity

A risk culture that prioritizes cybersecurity ensures that employees are vigilant, systems are secure, and incident response plans are in place. Proactive cybersecurity management prevents costly breaches, protects data, and thereby maintains members' trust and loyalty. Regulators are also paying close attention to how cybersecurity incidents are managed. A credit union with a strong risk culture is better prepared to meet regulatory expectations and safeguard its reputation in the event of a breach.

4. Climate change

Credit unions are not immune to the financial impacts of climate change. A strong risk culture ensures that environmental risk is incorporated into lending and investment decisions. It also ensures preparedness for potential financial industry reporting requirements related to climate risk disclosures. A risk-aware culture can better respond to the increasing frequency of natural disasters by considering forward-looking strategies to mitigate these impacts.

Implementing Risk Culture as the Foundation of ERM

An effective risk culture requires a proactive approach to enterprise risk management, which is grounded in several interwoven elements. When each element is operating effectively, the organization is better positioned to withstand headwinds. The figure below presents a visual of the key components that, when operating in concert, are the bedrock of a strong risk culture.

- Business Strategy:

The objective of a business strategy is to knowingly take risks to achieve the goals (financial and otherwise) of the credit union and its membership. The first step for an organization that has a strong risk culture is to establish and clearly articulate the link between its business strategy and enterprise risk management. This clarity ensures the risks emanating from its strategy are well understood, communicated, and managed for long-term viability. This alignment requires balancing risks (both known and potentially emerging risks) with expected rewards. As a credit union develops its strategic plan, the planning process should identify the risks that the plan may give rise to under different macroeconomic scenarios but also under various potential threat environments, such as failures due to privacy or cybersecurity breaches, third-party arrangements, or other external factors not immediately under the leadership and board's direct control.

- Risk Appetite and Risk Tolerance:

Once the strategy is well defined, the board and leadership team should determine the appropriate "risk appetite" that can be assumed in order to deliver on its business strategy (e.g., mergers, member growth, diversification, product mix, etc.). For example, if the strategy is focused on aggressive commercial loan growth, the risk appetite may lead to a willingness to accept higher credit risk, provided controls and robust, timely monitoring standards are in place to signal adverse changes in portfolio quality and prevent undue losses.

Risk appetite therefore refers to the amount and types of risk that an organization is willing to take to achieve its objectives.

On the other hand, risk tolerance defines the upper limit of risk taking that the organization can bear to take for each specific risk category such that it remains well capitalized.

In this respect, the board approves risk appetite statements for each major risk type after due discussion and review of challenging yet plausible scenarios. These risk appetite statements outline the credit union's overall willingness to take risks across its operations in pursuit of its strategy. Management then establishes supporting sub-risk limits for specific activities to prevent excessive risk taking in the achievement of its business goals.

The risk appetite statement and accompanying risk framework should be reviewed at least annually to determine whether adjustments are required due to changes in the operating environment, business activities, markets, and/or macroeconomic conditions. This could be part of the strategic planning cycle or occur more frequently, depending on any material changes. To close the loop, regular monitoring and reporting through a direct reporting relationship to the board should be established to measure performance against the accepted risk appetite.

- Risk Oversight and Governance

Credit unions should have robust corporate governance policies and processes covering, for example, corporate culture and values, strategic direction and oversight, organizational structure, the control environment, a suitability assessment process, board and senior management responsibilities, and compensation practices.

Credit unions should also perform an assessment, as required, of whether the existing governance framework is fit for purpose—e.g., a technology committee may need to be established due to shifting trends toward digitalization and heightened risks related to cybersecurity. It is important that these accountabilities and ownership be clearly established. This includes documenting and communicating the specific accountabilities of the board and its committees, senior leadership, the risk management committee, and ultimately, all employees.

Accountability at the Board includes the need for education and training on key risks and emerging risks affecting the credit union. The Board ensures its membership comprises individuals with a balance of skills, diversity and expertise, who collectively possess the necessary qualifications commensurate with the size, complexity, and risk profile of the credit union. It also includes practices that promote Board independence and renewal.

The Board approves policies that establish and communicate corporate culture and values, such as the code of conduct, and the conflict of interest policy. The Board oversees the design and operation of credit unions' compensation systems and related performance policies and procedures. As well, a strong risk culture ensures that an independent internal audit function conducts a periodic review of the effectiveness of risk oversight at key points along the risk oversight continuum.

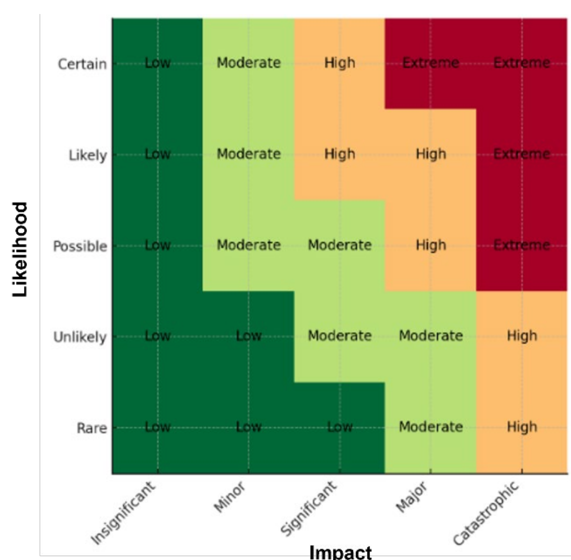
- Risk Data, Measurement, and Analysis:

Without question, data integrity is essential. It should be auditable and can be replicated. Presentations to the board should be clear, leverage visual aids, focus on a forward-looking assessment of potential risks, and prioritize and rank emerging risks. It is important to ensure that reassessments are conducted on an ongoing basis in response to

the evolving economic environment. Techniques for risk measurement may include a variety of options:

- Use a traffic light system of green, amber, and red to denote the extent of risk taking, as well as a graphical illustration of likelihood (probability) and severity (downside impact).
- Assess financial risks (credit, market, and liquidity) using quantitative analysis such as stress testing and scenarios involving varying degrees of severity.
- Assess operational, repetitional, and resilience risks using risk rating scales.

The ultimate objective is to prioritize risks based on their potential impact on financial stability and regulatory compliance, with a focus on high-probability and high-impact risks. For example, on the following heat map, red and potentially yellow would be priority focus areas.



- <u>Risk Mitigation:</u>

Once risks have been measured, assessed, and prioritized, strategies related to the management and mitigation of identified risks should be developed and approved, including the transfer of risk to third parties through hedging in the case of interest rate risk, or insurance for operational risks. For example, credit risk is managed by implementing credit approval guidelines, concentration limits, and underwriting guidance to ensure the organization stays within its approved risk appetite under differing economic scenarios. Contingency plans, incident response plans, and disaster recovery plans should be prepared, along with related playbooks, and mock tabletop exercises executed periodically at the leadership and board levels to prepare for worst-case scenarios, such as financial turmoil or an operational disruption.

- <u>Internal Controls:</u>

As previously documented in Stabilization Central's Lessons Learned series (Risk Management and The Three Lines Model), an internal control discipline is a key component of a strong risk culture. Internal controls start with "the tone at the top" and ensure there is separation of duties across the business, support functions, and internal audit. In an organization with a strong risk culture, "the tone at the top" is said to result in "an echo at the lower levels," implying that the emphasis on doing the right thing permeates the organization. Best practices underpinning internal control include, but are not limited to, a risk-based approach to assessing and analyzing risk, strong IT access controls, data validation and data integrity controls, a whistleblower mechanism, and real-time monitoring of suspicious/unusual lending approvals.

- <u>Risk Tools:</u>

Risk culture best practice recommends using a variety of tools and exercises to probe the effect of downside risks for the most important portfolio exposures (e.g., mortgage and commercial lending) emanating from adverse economic conditions. These tools may include scenario planning, stress testing, and table-top executive and board level exercises to simulate extreme but plausible events. At the same time, being prepared for and resilient to severe but plausible scenarios such as a privacy breach, a cyber event, or a third-party mishap requires that leadership and boards develop and maintain playbooks for tabletop exercises and that these playbooks are periodically tested.

- Monitoring, Reporting, and Communication:

A strong risk culture is aided by monitoring risk on a timely basis and escalating quickly when there is a misalignment between risk-taking activities and the established risk appetite. The areas of greatest financial risk, such as credit risk, liquidity, and market exposure, require the most accurate monitoring tools, but given the digital threat landscape, it is important to ensure ongoing scanning for cyber-related concerns. Deploy presentation formats that are easy to understand, actionable, and facilitate decision making as risks are reported up the line to management and the board. Dashboards and visual trend reports are recommended to highlight key risk indicators and key performance indicators for leadership and board reporting.

- People:

While all the above are critical elements, the ultimate test of a strong risk culture is evidenced by encouraging a safe "speak up environment," creating transparency, respectful communications, and a shared understanding of risks to the organization. One key aspect of risk culture is engagement through training for staff at all levels so that everyone understands what the risk policies are meant to achieve, what compliance with regulatory requirements means, and how to look out for emerging risks. Finally, risk cultures require that employee incentives be aligned with prudent risk taking as well as compliance with risk management policies.

Conclusion

By embedding a strong risk-aware culture into every layer of the organization, credit unions can be resilient, protect members' interests, and ensure long-term sustainability. The proactive and structured approach to managing risk outlined above not only safeguards against unexpected risk of loss but also helps maintain the credit union's reputation while promoting a culture of transparency, accountability, and ownership. In the context of current pressures on earnings, capital adequacy, and the rise of complex risks such as cybersecurity and climate change-related incidents, a strong risk culture and the key elements of this framework serve as a strategic differentiator for credit unions, promoting member retention, member trust, and financial stability.

What are the keys to embedding a risk culture?

- Ensure management models the desired risk culture.
- Include risk and compliance perspectives across the organization (through a Code of Ethics).
- Encourage and reinforce a "speak up" culture, including a whistleblower mechanism.
- Survey employees to ensure the tone from the top resonates at all levels and there is an echo at the bottom.
- Review the compensation structure to align incentives (e.g., promotions and remuneration) with prudent risk-taking to ensure risk culture permeates the entire organization.
- Ensure there is consequence management for misconduct behaviours.
- Make risk-based decisions that align with the organization's risk appetite.
- Ensure the stature and strength of internal controls and the three lines of defence.
- Have established and respected escalation protocols for breaches.
- Engage in oversight and reporting to management and the board of directors.

In contrast, a strong risk culture can be weakened by several factors that undermine risk management efforts, reduce transparency, and create an environment where risks are not properly identified, openly discussed, escalated, and actioned. Credit unions, like any financial institution, must guard against these detrimental influences, which can lead to poor decision making, regulatory non-compliance, operational disruptions, and financial loss.

Top Five Detractors From a Strong Risk Culture:

- **Leadership support is weak or lacking:** The tone at the top is crucial. If the board of directors and senior management do not prioritize or model good risk management practices, their inaction sends a message to

the rest of the organization that risk management is not important.

• **Misaligned incentives:** If employee incentives are based solely on rewarding short-term performance (e.g., loan volumes, revenue growth) without regard for risk, excessive risk taking may result. Likewise, incentives that reward high sales, aggressive targets, and rapid growth, but without appropriate risk controls, can push employees to bypass or ignore risk protocols, which can then result in operational and financial exposures.

• **Inadequate risk training and poor communication**: Without regular training on risk management and internal controls, employees may not understand how their actions contribute to the credit union's overall risk profile and can create blind spots. A strong risk culture requires continuous learning and adaptation to emerging risks.

• **Limited board oversight**: If the board does not actively engage in risk oversight, it signals that risk management is unimportant. Boards that do not have members with risk management expertise may not challenge risk-related decisions or ask the right questions to provide effective oversight. Strong board oversight is critical to instilling a robust risk culture.

• **External pressures**: External factors such as an economic downturn, a competitive landscape, or pressure to grow membership or earnings can result in excessive risk taking. A strong risk culture helps guard against decisions that compromise long-term sustainability. Likewise, if regulatory requirements are viewed solely as checklists, rather than as integral to sound risk management, this attitude can detract from a robust risk culture.

By continuously nurturing a risk culture that promotes transparency, tone from the top, board engagement, accountability, and a proactive approach to managing existing and emerging risks, our system can maintain a culture that supports long-term stability and resilience, even in challenging environments.

In closing, this paper has endeavoured to share guidance on how risk culture is the foundation of a sound and prudent approach to enterprise risk management. Regulatory expectations continue to increase, and the public has become less tolerant of financial mishaps. With technology and regulation rapidly evolving, it is important to ensure the appropriate risk culture is in place throughout your organization and at the board level, to maintain confidence in our credit union system and ensure our institutions' resilience.

Appendix A

Enterprise Risk Management Oversight – Regulatory Focus Areas

Boards and credit union executives are expected to have a deep understanding of risk management practices and oversee enterprise risk management (ERM) frameworks. The following are risk management areas of focus in the current environment.

1. **Enhanced ERM frameworks**: Credit unions are expected to have robust ERM frameworks that not only identify, measure, and mitigate risks but also have a direct and explicit link to the business strategy and its successful execution. These frameworks must align with the credit union's risk appetite and regulatory standards.

2. **Cybersecurity and operational resilience**: As members of the credit union system continue to expand their digital presence and products/services, it is critical to establish operational resilience, including robust cybersecurity practices, data protection, and business continuity planning. It is important to note that cybersecurity threats are not limited to large organizations, and a cybersecurity event may impact any member of our credit union system.

3. **Climate risk and sustainability**: Increasing attention is being paid to how climate risk may affect credit unions; this is a known risk, with geographic concentration issues close to home in BC as well as across the country. Credit unions need to incorporate environmental, social, and governance (ESG) risks into their risk assessment processes, analyses, board reporting, and decision making. The link between strategy execution and ESG risk governance is an important board-level topic.

4. **Capital and liquidity requirements**: Credit unions are expected to maintain adequate capital buffers and liquidity to weather financial shocks related to areas of credit risk concentrations (e.g., mortgages, commercial lending). If a certain product or business activity has a disproportionate impact on the financial health of a credit union, then one can reasonably expect additional regulatory focus on that area of risk taking. The stress testing of these metrics is becoming more rigorous, and there is a need to assess and demonstrate resilience under various challenging but plausible adverse conditions.

5. **Anti-money laundering and compliance:** Enhanced regulatory scrutiny regarding anti-money laundering practices requires that credit unions maintain strong compliance frameworks. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) governs these efforts. It is not sufficient to simply have policies and procedures in place; rather, there needs to be documentary evidence that these procedures are tested and gaps escalated, reported, and actioned such that the organization complies. The heightened focus on this area of risk has stemmed from certain recent high-profile incidents that resulted in severe regulatory penalties.

6. **Third-party risk management**: The reliance on third parties poses additional risk to the credit union system due to consequences that may arise from potential failures by external vendors and service providers for outsourced activities, including data management and payment processing. Reliance on these third parties may introduce risks such as operational disruptions, cyber threats, and privacy breaches, resulting in reputational risk.

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