**Enterprise Risk Management (ERM) Policy**

Description

This Policy outlines the directives made by the Board of Directors (Board) of *[[CUName]]* (Credit Union) to maintain the safety and soundness of the Credit Union and its Members’ assets through a comprehensive Enterprise Risk Management (ERM) program

**Purpose**

The purpose of the Credit Union’s ERM program is to identify, manage and monitor organizational risks and risk-related opportunities, both internal and external. The Board understands that effective risk management is a key driver to the long-term and sustainable success of the Credit Union. The scope of the Credit Union’s ERM program extends over the entire Credit Union and applies to all Credit Union functional areas, major processes, systems and third-party vendors.

**Authority**

This Policy is adopted by a majority vote of the Board pursuant to the Credit Union’s Bylaws.

**Definition & Goals**

ERM is defined by COSO[[1]](#footnote-1) as “a process effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

The goal of the Credit Union’s ERM program is ultimately to maximize potential gains and minimize potential losses. By adopting an ERM framework, the Credit Union will create a consistent, standardized, and scalable approach to risk management that will be applied across the entire Credit Union. The process identifies major risks and risk-related opportunities within the business and allows Senior Management to prioritize and identify critical risks. The ERM program is Credit Union-wide, and its overarching goals are to:

* Identify both emerging risk-related opportunities and risks to maximize potential gains and reduce costs and potential losses Credit Union-wide.
* Build a framework for current and future risk identification and assessment across the Credit Union
* Enable Senior Management to identify opportunities to improve consistency and performance Credit Union-wide.
* Establish clear ownership over risk areas, along with audit trails to investigate potential risks.
* Understand the relationship between key areas of risk and learn which risks are systemic.
* Allow the Board and Senior Management to understand how risks and risk-related opportunities might impact the Credit Union’s strategic goals and objectives.
* Establish an organized culture which prioritizes risk management and adds value to the Credit Union.

The ERM process deals with all of the various categories of risk associated with Credit Union’s business including credit, interest rate, liquidity, transaction (operating or fraud) compliance, reputation and strategic. *[[Note: While the NCUA Risk-Focused Examination Program does not include Technology/Cybersecurity Risks and Governance Risks, Quantum Governance encourages credit unions to track these risks as well.]]*

**Risk Profile**

The Credit Union’s risk profile (often called appetite) represents the levels of risk acceptable to the Board, CEO and Senior Management. The risk profile reflects a credit union’s willingness to take risks as they relate to its strategic organizational goals.

Risk Profile Statement

The Credit Union will take risk in the pursuit of strategic success, but only if these risks:

* *[[Insert your credit union’s risk profile statement. See sample below.]]*
* *Align with the Credit Union’s overall growth strategy; and*
* *Allow the Credit Union to maintain an acceptable Net Worth ratio as set forth by the Board and as required by the NCUA.*

The Credit Union’s risk appetite overall is *[[INSERT]].* Based on *[[INSERT NAME OF REGULATOR AND DATE]]* Examination of the Credit Union, the *[[INSERT NAME OF REGULATOR]]* rates the Credit Union as having *[[INSERT]]* risk.

*[[SAMPLE]]*

|  |  |  |
| --- | --- | --- |
| **Risk Factor[[2]](#footnote-2)** | **Credit Union Rating** | ***[[INSERT NAME OF REGULATOR AND DATE]]* Rating** |
| Credit  | Moderate | Low |
| Interest Rate  | Moderate | Low |
| Liquidity | Moderate | Moderate |
| Transaction | Low | Low |
| Strategic | Moderate | Low |
| Reputation | Low | Low |
| Compliance | Low | Low |
| Cyber Risks | Moderate | N/A |
| Governance | Low | N/A |
| Climate | Low | N/A |

**Risk-Based Approach**

The Credit Union will use a five-step process for risk management:

1. Identify and create a list of risks that have or could have an impact on business issue at hand.
2. Assess the risks by identifying sources/root causes of the risks, evaluating the impact and likelihood of the risks and account for mitigation or activation strategies.
3. Evaluate and determine which risk opportunities deserve mitigation and which deserve activation strategies.
4. Establish activities to either mitigate or seize upon (activate) the opportunities presented by the risks identified and evaluated in the previous steps.
5. Monitor the mitigation or activation activities.

**Responsibilities**

The Credit Union’s ERM program will support the Credit Union’s strategic priorities by:

* Continually assessing the risk exposures throughout the Credit Union.
* Performing an annual formal enterprise risk assessment and presenting the results of those assessments to the Board.
* Managing a quarterly process to identify key emerging risks, assess their potential impact on the Credit Union and reporting the results of the identification process to the Board.
* Working with key functional areas of the Credit Union to update the risk assessment results and address key risk responses on a routine basis.
* Ensuring that the Credit Union’s various planning processes consider the risks of key products, processes and strategies.
* Assisting in setting and monitoring risk tolerances for the Credit Union’s significant risks.
* Working with the Credit Union’s training department to conduct periodic ERM training.

**Board of Directors**. The Board approves the Credit Union’s risk profile and oversees its ERM program. However, the risk profile will be developed in constructive partnership with the Credit Union’s *[[Supervisory/Audit]]* Committee, CEO and Senior Management during the strategic planning process. with oversight conducted by the *[[Supervisory/Audit]]* Committee. At a minimum, the Board will receive quarterly updates regarding the ERM program through the *[[Supervisory/Audit]]* Committee, or more often as necessary.

**Senior Management-Level ERM Committee**. Operational responsibilities to manage the Credit Union’s risk profile, on a day-to-day basis, are delegated by the Board to the CEO and Senior Management. The CEO will establish an ERM Committee composed of Senior Management who represent a broad cross section of the Credit Union’s functional areas and are familiar with the key issues facing the Credit Union. The ERM Committee will meet no less than quarterly to discuss key risk issues and identify and address emerging risks and risk-related opportunities.

***[[Supervisory/Audit]]*****Committee**. The *[[Supervisory/Audit]]* Committee will assist the Board in fulfilling its oversight responsibilities with regards to the Credit Union’s ERM program by overseeing the ERM practices of the Credit Union as a whole, in relation to identifying, assessing, monitoring and managing risk across the Credit Union, and providing an open and ongoing communication forum between Senior Management and the Board to discuss risk management, mitigation and opportunities. The *[[Supervisory/Audit]]* Committee shall have the responsibilities and duties set forth below, as well as other matters specifically delegated to the *[[Supervisory/Audit]]* Committee by the Board and outlined in its charter.

* Monitor, along with the Board, Board committees and Senior Management, through the ERM Committee, the Credit Union’s risks and risk-related opportunities and coordinate risk management efforts for the Credit Union. While first-line ownership of various broad risk categories will reside with the full Board, the *[[Supervisory/Audit]]* Committee's interest extends over all organizational risk types (see above).
* Evaluate risk identification, assessment monitoring and managing techniques employed by Senior Management and reported through the ERM Committee and ensure current methodologies remain commensurate with the Credit Union's size and complexity.
* Review, affirm and validate the Credit Union's risk appetite statement on an annual basis and approve any material amendments to the risk appetite statement by engaging Senior Management, through the ERM Committee, and ultimately the Board in an ongoing risk appetite dialogue as conditions and circumstances change and new opportunities arise.
* Monitor the Credit Union’s adherence to its risk appetite.
* Review and make recommendations around key risk reports, policies, risk limits and the risk mitigation plan in constructive partnership with Senior Management, through the ERM Committee.
* With Senior Management, through the ERM Committee, promote the linkage between risk management and the strategic planning process.
* Oversee Senior Management's processes, through the ERM Committee, regarding the proposal of new strategic endeavors, projects and services to ensure such endeavors are within the Board's risk appetite and risks are proactively mitigated or risk-related opportunities are acted upon.
* Review material operational risk events, including losses and near misses.
* Review the status of litigation activity.
* Review material vendor/third-party due diligence activities.
* Review and evaluate the Credit Union’s business continuity programs.
* Ensure that the Credit Union’s ERM program has strong commitment and leadership across the organization, spearheaded by the ERM Committee, with sufficient stature, authority and seniority that is independent from individual business units.

**Policy Review**

This Enterprise Risk Management (ERM) Policy shall be reviewed annually by the *[[Supervisory/Audit]]* Committee and then by the Governance & Nominations Committee to determine whether changes should be made.

**Board Authorization**

This Enterprise Risk Management (ERM) Policy was approved by the Board at a meeting dated: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Secretary of the Board | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date |

**Acknowledgement[[3]](#footnote-3)**

By my signature below, I certify that I have received a copy of the Enterprise Risk Management (ERM) Policy and have read, understood and agree to comply with its terms.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Name  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date |

**Quantum Governance** provides credit unions, corporations, nonprofits, associations and governmental entities with governance and strategic consulting, facilitation and assessment. The firm is a unique L3C organization that integrates the best of the for- and non-profit communities into one practice. It is a low-profit, limited-liability service firm dedicated to the public good. This document is not intended for wide distribution nor to be relied upon for any purpose beyond its intended scope as an example Board policy. We are not providing legal services or offering legal advice of any kind. Please consult legal counsel in approving all governing documents. **Learn more at quantumgovernance.net.**

Do not copy, distribute or post without consent from Quantum Governance, L3C.
© Quantum Governance, L3C

1. COSO or the Committee of Sponsoring Organizations of the Treadway Commission is a voluntary private-sector organization dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on
in-depth research, analysis and best practices. [↑](#footnote-ref-1)
2. Note that the NCUA’s “risk-focused examination and supervision process identifies…seven [areas] of risks…” ([https://publishedguides.ncua.gov/examiner/Content/ExaminersGuide/Examination&SupervisionContacts/Risk-Focused\_Exam/Risk%20Categories.htm](https://publishedguides.ncua.gov/examiner/Content/ExaminersGuide/Examination%26SupervisionContacts/Risk-Focused_Exam/Risk%20Categories.htm)) which Quantum Governance has included on the table above. To those seven risks, we have added Cyber, Governance and Climate risks and strongly encourage credit unions to track their organizations’ risks in these critical areas as well. [↑](#footnote-ref-2)
3. Note: The Acknowledgement statement and signature block should be included on each Board-level policy (including job descriptions and committee charters) unless such policies are collected together in one Board-level governance policy manual. In such cases, one Acknowledgement statement and signature block will suffice for the entire governance policy manual and all of the policies contained therein. [↑](#footnote-ref-3)