

4711 Yonge Street
Suite 700
Toronto ON M2N 6K8
Telephone: 416-325-9444
Toll Free 1-800-268-6653
Fax: 416-325-9722

4711, rue Yonge
Bureau 700
Toronto (Ontario) M2N 6K8
Téléphone : 416 325-9444
Sans frais : 1 800 268-6653
Télécopieur : 416 325-9722



January 2018

Guidance Note:

Enterprise Risk Management (ERM)

All credit unions are required to implement a comprehensive Enterprise Risk Management (ERM) framework that is appropriately scaled to reflect its size, complexity and risk profile. An ERM framework includes the processes that the credit union uses to identify and manage significant risks and realize opportunities related to the achievement of their objectives. It involves an objective, pro-active enterprise wide view of all risks and their associated risk tolerances to ensure that they are fully aligned with corporate objectives and strategies, and reflect the quality, competencies and capacity of a credit union's human resources, technology and capital.

This guidance note, is for all credit unions and outlines the basic requirements for an enterprise risk management program.

It identifies the critical areas that will be considered in assessing the effectiveness of the credit union's ERM program as required under DICO By-law #5 - Sound Business and Financial Practices.

This document also outlines typical features of an ERM program and provides additional guidance on the responsibilities of the Board, Audit Committee (or other designated committee) and management in implementing an effective ERM program.

Further information is outlined in the ERM Framework and ERM Application Guide which are available on DICO's website.

Contents

Introduction 2

ERM Policy..... 2

Risk Appetite and Tolerances 3

Key Responsibilities 3

Reporting 4

DICO Expectations and Assessment Criteria 5

Introduction

Enterprise risk management (ERM) includes the methods and processes used by organizations to identify and manage significant risks. Significant risk is defined as an event or activity which may significantly or materially interfere with the achievement of an entity's goals or an event or activity which may cause a significant opportunity to be missed.

ERM is an iterative process. It provides a framework which typically involves a number of key steps including risk identification, risk assessment and measurement, risk response and action, monitoring and reporting, and application of lessons learned. By identifying and proactively addressing significant risks, credit unions can protect and create value for their stakeholders.

While the objectives are the same, there are many different approaches that may be considered for implementing an effective ERM program. Each has its own particular attributes and no one approach is necessarily better than the other. However, whatever approach is adopted, it is important that it is appropriately scaled to reflect the size and complexity of the credit union.

The board of directors plays a critical role in setting risk appetite and overseeing enterprise risk management systems, processes and practices. This responsibility requires an understanding of ERM processes and the nature and extent of risks facing the credit union.

A critical element in the risk assessment process is to identify and prioritize larger risks by severity in the context of the likelihood and impact of occurrence. While it is important for the Board to understand the breadth of risks facing the credit union, this process allows the Board to focus on the critical risks of the credit union.

ERM Policy

The ERM policy (policies) should outline the broad approach to risk management, key responsibilities and reporting requirements. It is also important to document how risks are identified, prioritized, assessed and managed and the nature and extent of reporting and oversight.

At a minimum, ERM policy should address the:

- risk appetite and risk tolerances of the credit union;
- key responsibilities of the Board, audit committee (or other designated committee), and management; and
- frequency, form and content of reporting requirements.

ERM Policies, including the risk appetite statement, should be reviewed at least annually.

Risk Appetite and Tolerances

Risk Appetite is the degree of risk on a broad-based level that a credit union is willing to accept or take in pursuit of its objectives. The credit union should outline an appropriate risk appetite statement that describes its overall approach to risk including any quantitative or qualitative attributes as appropriate.

Risk tolerance is the quantified level of risk that the credit union is willing to accept in various risk areas. Risk tolerances help evaluate and monitor significant risk exposures and the quality of risk management activities. Risks that fall materially outside of identified risk tolerances may indicate changes in external factors and/or ineffective risk management strategies that need to be addressed.

A credit union's risk appetite and risk tolerances should be influenced by its capacity to withstand adverse consequences. Risk appetite and risk tolerances are expected to vary based on the effectiveness of risk management processes and structures, the credit union's earnings capacity, and the level and quality of capital. A higher capacity to absorb adverse consequences provides a greater opportunity to adopt a higher risk appetite and set higher risk tolerances where appropriate. A lower capacity to absorb adverse consequences should be indicative of a much lower risk appetite and risk tolerances.

Key Responsibilities

The Board is responsible for:

- setting risk appetite levels
- overseeing ERM activities of the credit union;
- understanding the nature and magnitude of significant risks to which the credit union is exposed;
- reviewing reports on the assessment of risk levels compared to established strategic risk targets; and
- reviewing risk management policies annually, including risk appetite, and strategies to ensure that risk exposures remain appropriate and prudent.

The Audit Committee or other designated committee is responsible for:

- reviewing management's identification of the significant risks of the credit union in accordance with the ERM policy;
- ensuring there are enterprise risk management processes in place to measure, monitor, manage and mitigate significant risk exposures, including appropriate policies, procedures and controls;

- overseeing the application of ERM practices and the on-going identification of emerging risks; and
- reporting to the Board on risk exposure levels.

Management is responsible for:

- setting risk tolerance levels in line with the Board's approved risk appetite;
- identifying, measuring and evaluating significant strategic, business and process risk exposures;
- ensuring an appropriate level of resources are allocated in alignment with established risk appetite targets for assessing and managing risk;
- mitigating risk exposures through appropriate risk responses;
- monitoring the application of risk responses and mitigation strategies; and
- reporting ERM processes and findings, including the level and direction of risk exposures and extent of risk management activities.

Reporting

Reports are an important element to effective risk management and risk oversight. While there is no standard recommended ERM reporting format, it is important that reports clearly identify the risk profile of the credit union and the status of significant risks.

Reports should include information on the following:

- the nature and magnitude of significant risks and opportunities;
- highlight all significant risks and those risks that exceed their established risk levels;
- identify the timeframe and status of any additional risk management activities that may be required to bring risks within approved risk levels;
- identify any negative trends of higher risk areas and any changes to risk management activities;
- highlight any new risks including their risk assessment, risk response and management activities;
- identify any material emerging risks; and
- identify any exceptions to established policies or limits for key risks/risk areas.

In addition, the Audit Committee or other designated committee should report to the Board on its review of risk management activities, including the status of any significant current and emerging risk exposures and trends.

On a periodic basis, the Board should review all high-risk areas (even those that are appropriately mitigated within acceptable levels) in order to have a full understanding of all the significant risks facing the credit union.

DICO Expectations and Assessment Criteria

All credit unions are expected to adopt a prudent and disciplined approach to risk management. This includes implementing a robust ERM program that identifies and addresses all significant risk areas. As part of its on-going risk assessment process, DICO will assess the quality of ERM program and processes within the context of the credit union's size and complexity, and its risk profile and risk capacity. This will include consideration and review of the:

- level of Board understanding of ERM and the risk profile of the credit union;
- risk appetite and risk tolerances in relation to actual and projected earnings and capital;
- identification, measurement and oversight of significant risks and any emerging risks;
- content, quality and frequency of ERM reporting;
- extent and nature of Board discussion and review of ERM reports;
- oversight of action plans to address any residual high-risk areas; and
- aggregate risk in relation to earnings and capital.