Deposit Guarantee Corporation of Manitoba
La Société d'assurance-dépôts du Manitoba

Guideline

Subject: Enterprise Risk Management

Effective Date: July 1, 2022

Table of Contents

1.0 Overview

On July 1, 2022, DGCM issued new Standards of Sound Business Practice (SSBP) pursuant to s. 159.1 of *The Credit Unions and Caisses Populaires Act*. All credit unions and caisse (cu/caisse) must comply with SSBP that apply to them (s. 159.1).
The SSBP are available at this link:

https://web2.gov.mb.ca/laws/regs/annual/2022/089.pdf

The SSBP contain rules respecting cu/caisse capital, liquidity, investments, lending, and other matters. The SSBP also contain a set of principles that assist cu/caisse to direct and manage their institution in a prudent, effective, and appropriate manner. These are further defined in DGCM's **SSBP Guidance Framework**.

The Enterprise Risk Management (ERM) Guidelines better define DGCM's expectations on how a cu/caisse can comply with the SSBP, in particular Standard #3 – Risk Management.

These Guidelines draw upon standards published by other regulators in Canada and are not intended to be exhaustive.

Application to CUCM
DGCM is the prudential oversight body for Credit Union Central of Manitoba (CUCM). DGCM has issued Prudential Standards applicable to CUCM. These Guidelines also better define DGCM's expectations on how CUCM can comply with the Prudential Standards with respect to ERM.

2.0 Enterprise Risk Management

The objective of Standard #3 – Risk Management is to have a cu/caisse establish: "a comprehensive approach to identifying, managing, and controlling business and operating risks." Every cu/caisse must assume some degree of risk in its operations. A cu/caisse must develop strategies to manage those risks and take advantage of business opportunities.

Under the SSBP, the recommended risk management framework is ERM. In most Canadian deposit-taking jurisdictions, ERM is recognized as the best practice for managing risk. It allows a cu/caisse to analyze its risk enterprise-wide on an organized basis rather than on a fragmented (e.g. division by division) and *ad hoc* basis.

ERM is defined 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."
>
> Committee of Sponsoring Organizations (COSO)

ERM should integrate risk management and strategic management processes. A cu/caisse's ERM process will vary depending on its size, complexity, and nature of its risk. A well-integrated ERM process will enable a cu/caisse to identify and evaluate its risks and determine appropriate responses to those risks.

3.0 Governance Standards

3.1 ERM Policy: Role of Board and Management

Every cu/caisse should implement an ERM Policy. This policy should include an appropriate risk management philosophy and description of the ERM process. It should also clarify the roles, responsibilities, and accountabilities in the cu/caisse under the ERM process.

In order to meet board responsibilities under the Standards, the board should:

- Understand the key risks facing the cu/caisse and evaluate these risks regularly.
- Approve and regularly review an ERM Policy.
- Approve and regularly review appropriate and prudent risk management policies.
- Confirm that the cu/caisse has an appropriate and effective ERM process and oversee that process.

The board plays an important oversight role in confirming that management is monitoring and managing risks according to established risk tolerances.

The SSBP state that it is the responsibility of senior management to develop and drive the ERM process including:

- Develop and implement the ERM Policy, framework, and process.
- Identify risks, assess the significance, and determine a method for measuring and reporting those risks to the board.
- Provide the board with appropriate information on key or emerging risks.

3.2 Risk Management Philosophy & Appetite

The Standards state that a cu/caisse's risk management philosophy is at the core of a comprehensive ERM program. Every cu/caisse has an established culture and approach to risk: documenting this approach in the ERM Policy can guide the ERM process.

The risk management philosophy can be an introductory statement within the ERM Policy that defines a cu/caisse's risk culture and approach to identifying and dealing with risks. A well-defined risk management philosophy will help ensure that risk management is an integral part of all cu/caisse activities.

Once a risk management philosophy is defined, a cu/caisse should set a risk appetite for each of its key business risks.

A risk management philosophy may include objectives. For example, these could include:

- ERM will be integrated into the culture and strategic decision-making of the cu/caisse.
- The ERM process will anticipate and respond to emerging risks and changes to the business environment.
- ERM will balance the cost of managing risk with anticipated benefits.
- The board and senior management will raise awareness of the need for risk management.

3.3 Risk Tolerance

When establishing the basic framework for an ERM process, a cu/caisse should identify its risk appetite and set risk tolerances for all key business risks.

A risk tolerance describes a measure of risk, in quantitative terms, which a cu/caisse is willing to accept in individual risk categories. For example, a risk tolerance for credit concentration risk could be set using defined categories, such as “low”, “moderate”, or “high”. Depending on how these risk categories are defined, the tolerance set by the cu/caisse will help guide the management of the risk.

Regardless of the method used, DGCM expects a cu/caisse to compare actual risk exposures to its risk tolerances. A risk exposure that falls outside of a risk tolerance may highlight the need for management strategies to address the concern.

A cu/caisse’s risk tolerances are related to its ability to absorb risk or loss. If risk management processes are robust (as determined throughout the ERM process), and if a cu/caisse’s key financial indicators (e.g. capital, liquidity, profitability) are healthy, it may be able to accept higher tolerance levels for specific risks. Tolerances should be adjusted if financial indicators and risk management processes materially change.

3.4 Training and Expertise

A cu/caisse should consider what level of experience and expertise the directors, as a whole, should possess. The board of a cu/caisse should collectively understand the key risks facing their institution and the ERM process. Appropriate resources, including resources for training, should be provided to assist the board in fulfilling its mandate.

Senior management should have a strong understanding of the ERM process. Use of external resources and third party consultants may assist both senior management and the board if gaps are identified, particularly if a new ERM Policy and process is being developed.

4.0 ERM Process

4.1 ERM Process

The ERM Policy must define a clear risk identification and reporting process that involves senior management reporting to the board.

ERM should be a continuous, comprehensive, and integrated process. The process can range from simple to highly complex. When first developing an ERM process, a cu/caisse may benefit from using outside experts. However, accountability for managing the process remains with senior management.

Many ERM processes involve these five components:

- Risk Identification
- Risk Assessment and Measurement
- Risk Response and Action
- Reporting
- Monitoring

These five components of the ERM process should be documented to ensure that there is appropriate follow-up and continuity.

Risk Identification

Risks should be identified on an ongoing basis. When establishing a framework and setting risk tolerances, a cu/caisse may wish to create defined groups or categories of risk. Main risk categories often include: strategic, credit, financial/market, operational, and compliance risks.

For most cu/caisse, risk categories and identified risks within those categories will not change from year to year. However, all identified risks should still be regularly reviewed to ensure that emerging risks are captured.

Risk Assessment and Measurement

On a regular basis, as established under the ERM Policy, management or a committee of management/staff should meet to review all identified risks and assess whether risks have changed from the last assessment. Operational responsibility should not be delegated below the senior management level.

Many ERM processes assess and measure risk by looking at the likelihood an event or condition could occur and the impact such an event or condition will have on the cu/caisse.

Risk Response and Action

The person or group responsible for assessing and measuring risks should also provide recommendations on how to deal with the risk. Recommendations, as stated in the Standards, can range from accept to avoid.

Accept: The cu/caisse decides to accept, manage, and monitor the risk. It will not take action to reduce the risk.

Mitigate: The cu/caisse is willing to accept some risk by implementing control processes to manage the risk within established tolerances.

Transfer: The cu/caisse chooses to transfer the risk to a third party (e.g. obtaining insurance or hedging).

Avoid: The cu/caisse determines the risk is unacceptable and will eliminate those activities that give rise to the risk (e.g. cease selling a product, wind down a subsidiary, or reduce lending in a specific market).

Accountability for deciding how to address an identified risk, particularly one outside of tolerance, rests with the board.

Reporting

The board or a committee of the board will require regular reporting to meet its oversight function. This will provide assurance that risks are being managed within approved risk tolerances. At a minimum, ERM reports to the board or a committee of the board should:

- summarize the nature and status of key business risks
- highlight those risks that exceed approved risk tolerances
- highlight the status of risk management activities required to bring risks within approved risk tolerances
- identify material changes from the last report
- identify new or emerging risks

The use of reporting tools such as dashboards and heat maps may be beneficial.

Monitoring

Throughout the ERM process, risk responses should be monitored by the responsible manager to ensure that risks remain within risk tolerances.

When a risk falls outside of an acceptable risk tolerance, appropriate action should be taken to bring the risk back within tolerance. The board should ensure that it receives action plans and follow-up reports to monitor performance.

4.2 Strategic Planning & Internal Audit

A benefit of establishing an integrated ERM process is that the board will understand the key risks facing the cu/caisse for consideration at its annual strategic planning session. On an on-going basis, the cu/caisse should evaluate the potential impact of key risks on its corporate objectives.

A mature ERM process will ensure that organizational initiatives respond to, or are linked to, risks identified under the ERM process.

An added benefit to establishing an integrated ERM process is that regular identification and assessment of risk can complement the internal audit function of the cu/caisse. For example, when an Internal Audit Plan is approved, the audit committee should consider whether the Plan addresses key risks identified in the course of the ERM process.

4.3 Differential Requirements Based on Size and Complexity

Every cu/caisse is expected to adopt an ERM Policy and implement an ERM process. The complexity and resources dedicated to this process will vary among cu/caisse depending on their size, complexity, and level of risk.

Recognizing that the members of the cu/caisse Systems vary considerably, these guidelines differentiate between “small” (<$200 million), “medium” ($200 million to $1 billion), and “large” (>$1 billion) institutions based on asset size. Differentiation based on size provides initial parameters; however, DGCM’s expectations may vary if a cu/caisse has a complex business model.

Small institutions: A non-complex or simplified ERM framework may be appropriate for small institutions.

At small institutions, the CEO would typically be assigned the operational responsibility for the ERM process. This includes identifying key and emerging risks, assessing those risks, and providing recommendations to the board for managing those risks.

Medium-sized institutions: This category covers a wide range of institutions, therefore DGCM's expectations for the ERM process will vary depending on the complexity of the cu/caisse.

DGCM's expectation is that the ERM process will be formalized and robust. The operational responsibility for the ERM process may be assigned to the CEO or another senior manager. However, as the cu/caisse becomes larger and more complex, additional staff should be included in the process. This may be an internal team/ERM committee, one that should include a senior manager or the CEO. The process itself should also mature, including the use of more advanced measurement systems.

At the board level, a committee may be responsible for overseeing the ERM process. Currently, among some cu/caisse, the audit committee is assigned this role.

Large institutions: Once a cu/caisse reaches this size, DGCM expects that it will have a fully mature ERM process. The process will typically be guided by an ERM committee of staff/management that provides reports to senior management for review and recommendation to the board or board committee.