Ontario

Deposit Insurance Corporation of Ontario

Société ontarienne d'assurance-dépôts

STANDARDS OF SOUND BUSINESS AND FINANCIAL PRACTICES

ENTERPRISE RISK MANAGEMENT *Framework*

January 2018

Ce document est également disponible en français.

Notice

This document is intended as a reference tool to assist Ontario credit unions to develop an appropriate enterprise risk management framework. This document does not replace any provision of the Credit Unions and Caisses Populaires Act, the Regulations under that Act, or any other legal requirements applicable to Ontario credit unions. While DICO has made good faith efforts in preparing this document in accordance with DICO's statutory authority, DICO makes no representation, warranty or condition, express or implied.

Acknowledgement

We wish to thank the following individuals for their assistance in developing this material: Richard Adam (Northern); Martin Blais (Fédération des caisses Desjardins du Québec); Gay Chong (Windsor Family); Leo Gautreau (Meridian); Ron Hodges (Italian Canadian Savings); Gérald Morin (Alterna); Luc Racette (L'Alliance des caisses populaires de l'Ontario Limitée); Sandy Shaw (First Ontario); Julian Sellers (Kawartha); and Fay Booker (Booker and Associates).

Contents

Overview

Application

This document is intended to provide guidance on implementing an effective Enterprise Risk Management (ERM) program for all credit unions. This ERM framework should be used in conjunction with the ERM Application Guide. The basic principles outlined in these documents and the methodology and process adopted will need to be modified and appropriately scaled to reflect a credit union's size and complexity. This will include consideration of the range of products and services offered to **depositors**, capital structure, geographic coverage, business strategies and technology.

As a credit union grows in size and complexity the ERM program should evolve to ensure that all significant new, emerging and increased risks are appropriately considered and addressed as part of the on-going review and assessment process. When establishing an appropriate and effective enterprise risk management process, credit unions should give consideration to the guiding principles outlined in Appendix A.

Definitions

Risk is an event or activity that may have an impact on the credit union's ability to effectively execute its strategies and achieve its objectives or which may cause a significant opportunity to be missed.

Risk Management is an on-going process, involving the credit union's Board of Directors, management and other personnel. It is a systematic approach to setting the best course of action to manage uncertainty by identifying, analyzing, assessing, responding to, monitoring and communicating risk issues/events that may have an impact on an organization successfully achieving their business objectives.

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.

Risk Tolerance is the level of risk that the credit union is willing to accept in various risk areas. This can be measured in terms of both quantitative and qualitative dimensions.

Chief Risk Officer (if one is appointed) is normally identified as the person responsible to coordinate and oversee management of the ERM process and approve reports to the Audit Committee.

Introduction

Enterprise Risk Management is defined[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 the entity's objectives."

In summary, ERM:

- is a comprehensive, systematic, disciplined and proactive process that is used to identify, assess, manage and report on the significant strategic, business and process level risks related to the achievement of the credit union's objectives which are inherent in the business strategy and operations at any point in time;
- is a decision-making process for measuring and addressing any variation (positive or negative) from the credit union's desired objectives;
- forms a basis for the credit union's decision-making processes from the development of its strategy and objectives to its daily operations, reporting and compliance routines;
- provides the ability for management to make more efficient use/allocation of capital and resources within the organization to optimize capital levels;
- optimizes risk management by balancing the cost of risk with the cost of control for all aspects of the credit union's potential risk areas to ensure organizational objectives are met;
- is an integral part of sound business and financial management from the strategic planning process to the day-to-day operations of the credit union that helps identify and manage all material internal and external risks and opportunities that may affect its performance, reputation and viability;
- seeks to enhance value and preserve the longer-term viability of the credit union; and
- is a fundamental responsibility and accountability of the Board and senior management.

[1] Committee of Sponsoring Organizations (COSO) ERM Integrated Framework Document 2004

ERM involves a pro-active holistic enterprise-wide view of all risks and their associated risk appetite and tolerances to ensure that they are fully aligned with the credit union's objectives and strategies, and reflects the quality, competencies and capacity of people, technology and capital. ERM also helps identify the interdependency and interaction of risks across the organization and provides the tools to rationalize risk management activities.

Purpose and Objectives

The purpose of ERM is to create, protect, and enhance member value and the credit union's viability by managing the uncertainties that could influence achieving its objectives. Implementing an effective ERM achieves the following key objectives:

Oversight: All critical risks have been identified and are being managed and monitored under a holistic approach consistent with the Board approved risk appetite statement.

Ownership and Responsibility: The ownership of risk is assigned to management individuals who are responsible for identifying, evaluating, mitigating and reporting risk exposures.

Assurance: The Board, management and depositors have reasonable assurance that risk is being appropriately managed within defined levels to bring value to the organization**.**

Benefits

A credit union which successfully implements ERM should expect the following benefits:

- More efficient use of capital and resources
- Reduced likelihood of operational loss
- Lower compliance/auditing costs
- Earlier detection of unlawful activities
- Fewer surprises
- Focus on lower cost prevention rather than higher cost resolution strategies
- Cost savings by using risk information to streamline and improve processes
- Increased awareness and integrated view of risks (existing and emerging)
- Systematic, repeatable approach to mitigate risks and identify opportunities

- Clearer, better informed decisions

By being informed, the Board and senior management can be proactive in responding to the significant risks and opportunities that the credit union experiences as a financial institution. ERM helps identify strategically significant high priority risk issues for the Board's attention. Through a comprehensive risk identification and assessment process, credit unions can identify who owns the risk and how best to respond to the risk. This ensures that the most appropriate and optimum level of resources is assigned to areas of greatest risk. Enterprise risk management helps identify opportunities as well as identifying risks. To be effective and not create additional overhead, ERM should be integrated into existing processes within the credit union that support such activities as strategic planning, business-planning, compliance monitoring, performance measurement and process re-engineering. Building ERM into existing processes increases awareness and sensitivity to risk and helps create a culture where risk is proactively assessed and managed at every level.

Roles and Responsibilities

The key roles and responsibilities of the Board and Management are summarized in Table A below.

TABLE A: Key ERM Roles and Responsibilities

The Board of Directors governs the risk profile of the Credit Union	Management takes action to manage the risks to an acceptable level
Oversees of ERM framework - gains assurance on its effectiveness	Develops processes to implement Enterprise Risk Management in the credit union
Establishes, approves, annually updates governing policy on Enterprise Risk	Assigns responsibilities for risk ownership, monitoring of risk, risk reporting
Articulates risk appetite/risk tolerance in policy	Identifies process to develop risk profile
Gains understanding of overall risk profile of credit union at inherent and residual levels	Implements processes to develop risk profile and to assess the severity of each risk
Gains understanding of significant risks at inherent and residual levels	Implements processes to determine risk responses are in place, and identify if further action required

Understands level of risk absorber (capital) in relation to aggregate residual risk of credit union	Determines level of risk absorber (capital) in place, make recommendations where it is not sufficient
Approves acceptance of residual risks or direct additional risk response action where residual level is in excess of established risk appetite/tolerance	Reports to Board on the risk profile of the credit union including significant risks at the inherent and residual level
Gains assurance that management has undertaken the risk responses as outlined	Takes action, monitors to ensure risk responses operate effectively and continuously
Monitors risk indicators for known significant risks on quarterly basis and more frequently on specific risks when issues arise	Presents periodic reports to Board which present risk indicators and level of risk by categories
Monitors emerging risks and discuss implications with management	Presents information to Board on emerging risks

The Process

ERM is an on-going and cyclical process. The Board and senior management set the tone for enterprise risk management in the credit union. This includes establishing the credit union's risk appetite and how risks will be identified, measured and managed.

There are five primary steps in the ERM process, as indicated in Table B. It is also important to ensure that ERM process and risks are re-evaluated and updated on an on-going basis to reflect new information and experiences so that all significant risks are appropriately identified and addressed and that any material opportunities are not overlooked.

TABLE B: Enterprise Risk Management Cycle

The process requires the involvement from all levels in the credit union and requires a willingness to understand the risk facing the credit union, assist with the creation of appropriate responses to risks, and maintain them within the risk appetite and tolerances established by the Board and senior management.

Risk Identification

Identification of risks should occur on an on-going basis for existing processes and on an ad-hoc basis as required for new product introductions, projects or changes contemplated to existing products and processes. There are several techniques that may be used to help identify risks including self-assessment questionnaires, surveys, workshops and interviews. To help with risk identification, risks should be considered within main risk categories such as strategic, credit, financial, operational and compliance risks.

TABLE C: Sample Main Risk Categories

Risk Assessment and Measurement

Risk assessment includes consideration of the likelihood of a risk occurrence and the impact of a risk on the achievement of the credit union's objectives within a specified timeframe. The likelihood of occurrence is often based on the probability or frequency (number of times) the risk might occur over a specified timeframe such as once a quarter, daily, twice a year, etc. A higher probability or frequency of the event occurring will result in higher risk weightings. An event that is expected to occur sooner rather than later will also result in a higher likelihood. The impact of occurrence is often stated as a dollar value of loss or percent of impact on earnings or capital, but can also be described in qualitative terms (e.g. reputation, service quality, regulatory compliance, etc.) that could result if the risk event occurred. The magnitude or severity of a risk is based on the product of its likelihood and impact.

Risk Response and Action

For each identified risk the credit union should establish an appropriate "response" option in order to optimize risk management. These generally range from accept to avoid. Four possible response options are identified in Table D below.

TABLE D: Sample Risk Response Definitions

Response	Definition
Accept	The credit union decides to accept, manage and monitor the level of risk and take no action to reduce the risk
Mitigate	The credit union is willing to accept some risk by implementing control processes to manage the risk within established tolerances
Transfer	The credit union chooses to transfer the risk to a third party (e.g. obtaining insurance)
Avoid	The credit union feels the risk is unacceptable and will specifically avoid the risk (e.g. cease selling a product or lending in a specific market)

Generally, if the magnitude or severity of the risk under consideration is high, the risk response needs to be strong (mitigate, transfer or avoid). Each risk and related response should be assigned to the manager who is responsible for the area affected by the risk. As part of the response process, management should determine and document what actions (prevention or detection) are necessary to manage the risk.

Monitoring

Risks and risk response activities should be monitored by the responsible manager to ensure that significant risks remain within acceptable risk levels, that emerging risks and gaps are identified, and that risk response and control activities are adequate and appropriate. Internal Audit and the Audit Committee (or other committee delegated to by the Board) play an important oversight role in confirming that management is monitoring and managing risks in accordance with established levels. Indicators that fall outside of acceptable risk levels should be escalated with appropriate action plans to bring the risk back within established risk levels. Those risks that still remain above acceptable risk levels should be considered by the Board for their approval of any necessary resolution strategies. This activity will form the basis for reporting to the Board and on-going monitoring by management.

It is also helpful to “quantify” the aggregate exposure of significant risks (or specified subset of risks) in terms of potential impact on capital. While this is often subjective and may be difficult to determine, it does help indicate any material change in risk levels from one period to another and could identify potential risks that may not otherwise be fully noted. It also helps to confirm that the level of aggregate risk exposure is within the established risk appetite of the credit union as established in policy.

Reporting

The Board, audit committee and senior management will require the results of the ERM process to be reported to them in their oversight capacity and to gain assurance that risks are being managed within approved risk levels.

At a minimum, ERM reports to the audit committee (or other designated committee) and/or

Board should:

- summarize the nature and magnitude of significant risks;
- highlight all significant risks and those risks that exceed their acceptable 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
- summarize any exceptions to established policies or limits for key risks.

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.

APPENDIX A: GUIDING PRINCIPLES

Guiding Principles

When developing an appropriate and effective enterprise risk management framework, credit unions should consider the following key guiding principles:

- Decisions should be made with appropriate consideration of the impact on the overall organization, not just the individual lines of business;
- The governance model should provide a forum for risks to be appropriately considered, discussed, debated, and factored into strategic business decisions;
- Governance should focus on and enable making risk management processes proactive rather than reactive;
- The risk governance structure should consider and reflect the roles and interaction with related functions, including compliance, internal audit, etc.;
- There should be a clear understanding of the requirements and appropriate resources to provide independent assurance (e.g. independent audit);
- The governance model must reflect separation of the three main areas of:
    - ✓ Business units that take risk and manage the risks they take;
    - ✓ Risk management that provides policy, guidance, recommendations, risk reporting and analysis; and,
    - ✓ Independent assurance functions such as internal audit.
- The risk governance model should evolve over time, as the credit union changes.

APPENDIX B: SAMPLE ERM POLICY

Purpose

The credit union will maintain a robust ERM framework to ensure:

- significant current and emerging risks and opportunities are identified and understood;
- appropriate and prudent risk management systems to manage these risks are developed and effectively implemented;
- regular reviews are conducted to evaluate the effectiveness of risk mitigation measures; and
- reports are produced on a regular basis regarding adherence to this policy

Objectives

The objectives of this policy are to:

- establish the risk appetite of the credit union;
- identify the key responsibilities of the Board, audit committee and management; and
- outline the frequency, form and content of reporting requirements.

Risk Appetite and Risk Tolerances

The risk appetite of the credit union is *[MODEST] [This should be defined by the credit union including quantitative and/or qualitative attributes.]* Significant risks must have Board approved risk management policies and/or risk management strategies.

Risk tolerances will be developed for each identified significant risk that reflect the level of risk appetite elected by the Board and management *[indicate what these are or how and where these are to be set out.]*

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
- annually reviewing risk management policies, 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 or the Chief Risk Officer] is responsible for:

- recommending risk tolerance levels to the Board;
- 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 of risk exposures through appropriate risk responses;
- monitoring the application of risk responses and mitigation strategies; and
- reporting on ERM processes and findings, including the level and direction of risk exposures and extent of risk management activities.

Reporting

Management will submit a report to the *[Audit Committee or other designated committee]* at least quarterly. The report should provide appropriate information on the following:

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

The *[Audit Committee or other designated committee]* will report to the Board on its review of risk management activities, including the status of any significant current and emerging exposures and trends.

ERM Review

The effectiveness of the ERM framework should be assessed from time to time including a review of all significant risks and the risk environment of the credit union. As well, any changes to the framework should be recommended to the Board of Directors.