SUPERVISORY LETTER

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF EXAMINATION AND INSURANCE
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: **November 7, 2013** **Supervisory Letter No.: 13-12**

TO: **All Field Staff**

SUBJECT: **Enterprise Risk Management (ERM)**

This Supervisory Letter discusses how NCUA views enterprise risk management (ERM) as one framework for managing risk and NCUA's supervisory expectations with regard to credit unions' risk management programs.

Natural person credit unions are not required to implement a formal ERM framework. However, credit unions are expected to have sound processes sufficient to manage the risk associated with their business model and strategies. This Supervisory Letter further explains that distinction and outlines what examiners should consider when evaluating the overall effectiveness of a credit union's risk management program.

Sincerely,

/s/

Larry Fazio, Director
Office of Examination & Insurance

Supervisory Letter

Enterprise Risk Management

1. Introduction

This Supervisory Letter provides examiners with an overview of the concepts and principles of enterprise risk management (ERM) as drawn from contemporary risk management practices. It also describes NCUA's supervisory perspective on ERM and outlines supervisory expectations regarding credit unions' use of a formal ERM framework.

2. What is Enterprise Risk Management (ERM)?

Enterprise risk management is a comprehensive risk-optimization process that integrates risk management across an organization. An organization's board of directors ultimately makes the decision to develop and implement an ERM framework, often with the goal of aligning risk with strategic objectives.

ERM is not a process to eliminate risk or to enforce risk limits, but rather to encourage organizations to take a broad look at all risk factors, understand the interrelationships among those factors, define an acceptable level of risk, and continuously monitor functional areas to ensure that the defined risk threshold is maintained.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defines ERM as a process that is:

- ongoing and applied throughout an organization,
- effected by people at every level of an organization,
- applied in strategy setting,
- takes an organization-level portfolio view of risk,
- designed to identify potential events that could affect the organization and to manage risk within the organization's risk appetite,
- able to provide reasonable assurance to an organization's management and board of directors, and
- geared to achieve objectives in one or more separate but overlapping categories.[1]

---

[1] See the Committee on Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management – Integrated Framework*, available at www.coso.org/documents/coso_erm_executivesummary.pdf. The COSO framework is widely recognized throughout the financial services industry as acceptable guidance on ERM. Another approach to ERM is discussed in "Risk management – Principles and guidelines" (ISO 3100:2009), which was published by the International Organization for Standards in 2009.

The *enterprise-wide* aspect of ERM is what differentiates it most fundamentally from more traditional risk management approaches. Many organizations, including credit unions, traditionally have used internal auditors to perform risk assessments and to report their findings to executive management and/or the Audit Committee. Under this approach, risks are considered and addressed individually, perhaps without consideration of the strategic implications these risks may impart or how the risks interrelate to one another. ERM reduces this silo effect and, at the same time, ensures ongoing communication with relevant stakeholders (board, senior management, audit, etc.).

3. Basic components of an ERM framework

There is no "off-the-shelf" solution for organizations seeking to launch an effective enterprise-wide approach to risk management. Rather, organizations can meet their specific needs with various tailored approaches that take into account their complexity, resources, and expertise. Credit unions that incorporate ERM into their risk management infrastructure may resource the program internally, through paid consultants, or through a combination of outsourced and internal resources. NCUA does not view any approach as preferable, provided core principles, controls, and due diligence are properly established within the organization. That said, there are several basic components of an ERM program that likely will be evident at any financial institution that pursues an ERM approach to managing risk. Because examiners are likely to encounter one or more of these components in their analysis of a credit union's operations, they should be familiar with them.

The table on the following page outlines these components (as identified in the COSO framework), describes each, and provides positive examples of how each component might manifest in a credit union's operations.

ERM Component	Description	Positive Example(s)
Established "Risk Culture"	This is the "tone at the top" that sets the basis for how risk is viewed and addressed by an organization's stakeholders at all levels. The organization should define an enterprise-wide philosophy for risk management and risk appetite that is grounded in integrity, ethical values, and a good grasp of how various stakeholders are affected by the organization's decisions.	• Consistent support for the ERM framework throughout the organization, from the Chairman's office to staff members on the front lines.
Clear Objectives	An ERM program encourages management to set clear strategic, operations, reporting, and compliance objectives that support and align with the organization's mission and are consistent with its risk appetite.	• Future objectives are reasonably achieved without exceeding a pre-determined, stated risk tolerance.

ERM Component	Description	Positive Example(s)
Event Identification	The organization has identified internal and external events affecting achievement of objectives and has distinguished its risks from its opportunities.	• For each uncertainty or potential event, a "leading indicator" is created along with parameters that would trigger a risk management response.
Risk Assessment	The organization continuously analyzes risk, considering the likelihood and impact of various scenarios, and uses the results of the analysis as a basis for determining how to manage those risks.	• A risk "heat map" evolves from manager surveys to determine priority of risks.
Risk Response	Management evaluates possible responses to risks, selects a response (avoid, accept, reduce, or share risk), and develops a set of actions that aligns risks with the organization's risk tolerances and risk appetite.	• Management identifies the costs and benefits for accepting each type of risk. • The most relevant risk information is centralized and reported timely, in the right form, and to the right people in order to make timely and effective decisions about risk.
Control Activities	A set of policies and procedures that is established and implemented to help ensure that an organization effectively responds to risks.	• Staff understands the differences between risk avoidance, risk reduction, risk sharing, and risk acceptance. • The senior manager responsible for ERM oversight reports directly to the board of directors or a board-established committee that will assure proper oversight and independence. • The ERM program is independent of the risk-taking and operational functions.
Information and Communication	Relevant information is identified, captured, and communicated in a form and timeframe that enable stakeholders to carry out their responsibilities. Key information about strategy and decisions is communicated clearly and broadly throughout an organization.	• All personnel receive a clear message from top management that ERM responsibilities are taken seriously. • A robust and reliable reporting regimen is evident.
Monitoring	The organization monitors—through ongoing management activities and/or separate evaluations—the entirety of risk management and makes modifications as necessary.	• Management reports performance versus established risk limits.

4. NCUA's supervisory perspective

Core ERM principles can be integrated into the overall strategic planning and organizational risk-management infrastructure of credit unions of all sizes and risk levels, and NCUA encourages credit unions to consider the benefits of doing so. However, implementing a formal ERM framework requires a significant investment in management, expertise, and systems.

NCUA recognizes that most credit unions do not possess the size, depth of resources, or range and level of risk exposures to warrant the significant investment necessary to implement such a program. Thus, NCUA requires that only corporate credit unions develop and follow a formal ERM policy.[2] ERM is not a regulatory requirement for natural person credit unions.

When examining smaller, less complex natural person credit unions, examiners should ensure the risk management framework is sufficient to manage the major risks present in the credit union's business strategy and objectives, understanding it needs to reflect a reasonable cost-benefit balance.

In large, complex natural person credit unions, examiners should ensure the credit union employs a comprehensive risk management approach, which may or may not include a formal ERM program. While any weaknesses in a large credit union's risk management processes will be addressed as supervisory concerns, examiners will not require credit unions to adopt a formal ERM program.

More details about NCUA's supervisory expectations with regard to risk management programs are provided below.

5. Addressing risk management in examinations

Part of the examiner's role is to gauge the effectiveness of all risk management programs against the identified and perceived risk posture of the credit union, the capability and commitment of management toward a culture of risk management, and the financial strength of the credit union in relation to individual and collective risk exposures.

In all cases, examiners are expected to take a risk-based approach to evaluating a credit union's risk management processes by considering:

- the credit union's risk posture, risk appetite, and risk management strategies;
- the depth and breadth of potential exposures including the types of products and services offered by the credit union;

---

[2] See NCUA Rules and Regulations Section 704.21 (www.ncua.gov/Resources/Pages/LCCU2013-02.aspx).

- the strategic objectives and operational policies, procedures, and controls in relation to potential exposures;
- concentrations of risk;
- risk-mitigating factors;
- capability and resources of management;
- current and historical performance management; and
- the financial strength of the credit union in relation to assets and activities.

Examiners are expected to employ the "total analysis process,"[3] which involves a comprehensive (enterprise-wide) risk assessment. This requires examiners to evaluate the range of risks and level of exposures, both financial and nonfinancial, to determine whether exposures are reasonable in relation to operational controls, decision support systems, policies, procedures, internal controls, and capital. Risks are then evaluated individually and collectively. Finally, examiners measure that risk in relation to CAMEL[4] and the seven risk factors.[5]

Examiners are expected to address poorly managed or excessive risk by addressing the underlying operational, strategic, and managerial deficiencies leading to unacceptable exposure. A DOR may be issued outlining underlying areas of unacceptable risk for which management does not have an adequate identification, measurement, monitoring, control, and reporting structure.

NCUA views the absence of an adequate risk management framework (ERM or otherwise) consistent with an institution's size, diversity, and depth of risk exposures as a failure in sound corporate governance, and expects examiners to take appropriate action consistent with the severity of the deficiency.

6. Conclusion

ERM is a broadly defined and evolving concept that, at its core, presents potential benefits to larger, more complex credit unions. Natural person credit unions are encouraged to explore how ERM might benefit their organization, but are not required by regulation or supervisory expectation to implement a formal ERM process. Examiners are encouraged to familiarize themselves with the concept and basic components of ERM to aid in their evaluation of a credit union's ability to identify, measure, monitor, and control (*i.e.*, manage) existing and potential risks in their operations.

---

[3] Chapter three of NCUA's Examiner's Guide (www.ncua.gov/Legal/GuidesEtc/Pages/Examiners-Guide.aspx) discusses the total analysis process in depth.

[4] **C**apital Adequacy, **A**sset Quality, **M**anagement, **E**arnings, and **L**iquidity/Asset-Liability Management

[5] The seven risk factors are credit risk, interest rate risk, liquidity risk, transaction risk, compliance risk, strategic risk, and reputation risk. (See NCUA Letter to Federal Credit Unions: Risk-Focused Examination Program (May 2002) available at www.ncua.gov/Resources/Documents/LFCU2002-09.pdf for more details.)