ACUIA
Association of Credit Union Internal Auditors

29TH ANNUAL CONFERENCE & ONE DAY SEMINAR

How ERM and Audit Work Together

Friday, June 21
10:45 am – 11:30 am

Presented By:
Robin D. Hoag, CPA, CGMA, CMC
Shareholder, Financial Institutions Group

Researched by:
Joseph A. Zito, CPA, MBA, Shareholder
Robin D. Hoag, CPA, CGMA, CMC

DoerenMayhew
CPAs AND ADVISORS

Internal Auditors – ERM Members

- How many of you have responsibility for ERM?
- How many have only responsibility for Internal Audit?
- How many of you are over $1 Billion?
- How many of you are under $500 million?

Overview of Discussion

- Seven risks NCUA expects credit unions to manage
- Background of Enterprise Risk Management (ERM)
- CEO/Manager's guide to ERM
- Components of ERM
- Benefits of ERM
- Questions

Seven Risks NCUA Expects Credit Unions to Manage

- Credit
- Interest rate
- Liquidity
- Transaction
- Strategic
- Reputation
- Compliance

NCUA Supervisory Letter 13-12

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]

NCUA Supervisory Letter 13-12

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.

ERM Component: Established “Risk Culture”

Description

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 grounded in integrity, ethical values, and a good grasp of how various stakeholders are affected by its decisions.

Positive example

For each uncertainty or potential event, a " leading indicator" is created, along with parameters that would trigger a risk management response.

Source: NCUA Supervisory Letter 13-12

ERM Component: Clear Objectives

Description

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.

Positive Example

Future objectives are reasonably achieved without exceeding a pre-determined, stated risk tolerance.

Source: NCUA Supervisory Letter 13-12

ERM Component: Event Identification

Description

Organization has identified internal and external events affecting achievement of objectives and has distinguished its risks from its opportunities.

Positive Example

For each uncertainty or potential event, a " leading indicator" is created, along with parameters that would trigger a risk management response.

Source: NCUA Supervisory Letter 13-12

ERM Component: Risk Assessment

Description

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.

Positive Example

A risk "heat map" evolves from manager surveys to determine priority of risks.

Source: NCUA Supervisory Letter 13-12

ERM Component: Risk Response

Description

Management evaluates possible responses to risks, selects a response (avoid, accept, reduce, share), and develops a set of actions that aligns risks with the organization's risk tolerances and risk appetite.

Positive Examples

- 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.

Source: NCUA Supervisory Letter 13-12

ERM Component: Control Activities

Description

A set of policies and procedures that is established and implemented to help ensure risks are effectively responded to.

Positive Examples

- Staff understands the differences between risk avoidance, risk reduction, risk sharing, and risk acceptance.
- Senior manager responsible for ERM oversight reports directly to the Board or a Board-established committee that will assure proper oversight and independence.
- ERM program is independent of the risk-taking and operational functions.

Source: NCUA Supervisory Letter 13-12

ERM Component: Information and Communication

Description

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.

Positive Examples

- All personnel receive a clear message from top management that ERM responsibilities are taken seriously.
- A robust and reliable reporting regimen is evident.

Source: NCUA Supervisory Letter 13-12

ERM Component: Monitoring

Description

Through ongoing management activities and/or separate evaluations, the organization monitors the entirety of risk management and makes modifications as necessary.

Positive Example

Management reports performance versus established risk limits.

Source: NCUA Supervisory Letter 13-12

Committee of Sponsoring Organizations (COSO)

- In 1992, COSO:
  - Established a common definition of internal control
  - Created Framework for evaluating the effectiveness of internal control
- In 2004, Framework was expanded to create ERM

Joint initiative of five private sector organizations

COSO Framework

- In 2013, a new Framework was created that:
  - Codifies principles supporting the five components of internal control
  - Clarifies the role of objective-setting in internal control
  - Reflects the increased relevance of technology
  - Incorporates an enhanced discussion of governance concepts
  - Expands the reporting categories of objectives
  - Enhances consideration of anti-fraud expectations
  - Increases focus on non-financial reporting objectives

Changing Risk Landscape

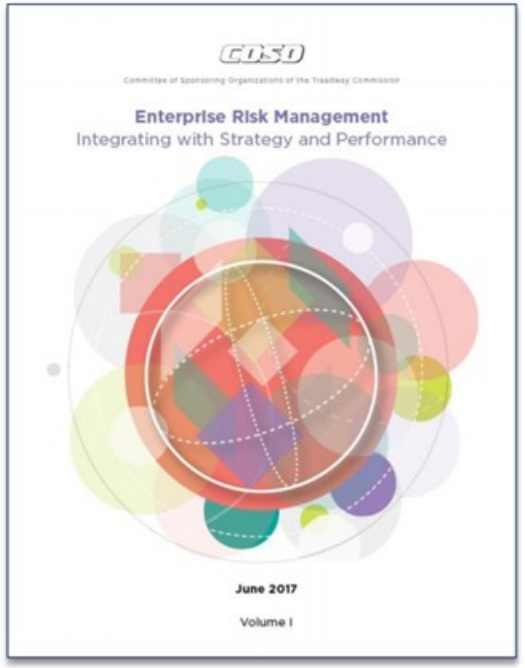
- Every choice we make in the pursuit of objectives has its risks.
- ERM may be called both an art and a science.
- Risk is considered in the formulation of an organization's strategy and business objectives.
- ERM helps to **optimize** outcomes.

Changing Risk Landscape

- The margin for error is shrinking.
- Credit unions encounter challenges that impact reliability, relevancy, and trust.
- Stakeholders are more engaged today, seeking greater transparency and accountability for managing the impact of risk while also critically evaluating leadership's ability to crystalize opportunities.

2017 Update to ERM Framework Issued September 2017

- Highlights the importance of ERM in strategic planning.
- Emphasizes embedding ERM throughout an organization, as risk influences strategy and performance throughout the organization.
- The first part offers a perspective on current and evolving concepts and applications of ERM to meet the demands of an evolving business environment.



Source: COSO 2017 Executive Summary

2017 Update to ERM Framework

- Organized into five easy-to-understand components that accommodate different viewpoints and operating structures to enhance strategies and decision-making.
- Focuses on challenges and evolving expectations of ERM that business leaders and boards are dealing with in today's landscape, including shifts in economic markets, evolving technologies, and changing demographics in supporting decision-making.

Source: COSO 2017 Executive Summary


ENTERPRISE RISK MANAGEMENT
Mission, Vision, and Core Values
Strategy and Business Objectives
Enhanced Performance
Risk Governance and Culture
Risk, Strategy, and Objective-Setting
Risk in Execution
Risk Information, Communication, and Reporting
Monitoring Enterprise Risk Management Performance

COSO Framework

2013

2004

Management's Guide to ERM

- Adding perspective to the strengths and weaknesses of a strategy as conditions change, and to how well a strategy fits with the organization's mission and vision.

Source: COSO 2017 Executive Summary

Management's Guide to ERM

- Allows management to feel more confident they've examined alternative strategies and considered the input of those in their organization who will implement the strategy selected.
  - Mergers
  - Incentive compensation systems
  - Loan products (member business lending, participations)
  - Commercial deposits/MSBs/MRBs
  - Internet banking

Source: COSO 2017 Executive Summary

A Focused Framework (2017)

The Framework itself is a set of principles organized into five interrelated components.

Source: COSO 2017 Executive Summary

Focuses on Integration

- Integrating ERM with business practices results in better information that supports improved decision-making and leads to enhanced performance.
- It helps organizations to:
  - Anticipate risks earlier or more explicitly, opening up more options for managing the risks
  - Identify and pursue existing and new opportunities
  - Respond to deviations in performance more quickly and consistently
  - Develop and report a more comprehensive and consistent portfolio view of risk
  - Improve collaboration, trust, and information sharing

Source: COSO

Emphasizes Value

- Enhances the focus on value: how entities create, preserve, and realize value
- Embeds value throughout the framework, as evidenced by its:
  - Prominence in the core definition of enterprise risk management
  - Extensive discussion in principles
  - Linkage to risk appetite
  - Focus on the ability to manage risk to acceptable levels

Source: COSO

Links to Performance

- Enables the achievement of strategy by actively managing risk and performance
- Focuses on how risk is integral to performance by:
  - Exploring how enterprise risk management practices support the identification and assessment of risks that impact performance
  - Discussing tolerance for variations in performance
- Manages risk in the context of achieving strategy and business objectives, not as individual risks

Source: COSO

Links to Performance

- Introduces a new depiction referred to as a risk profile that incorporates:
  - Risk
  - Performance
  - Risk appetite
  - Risk capacity

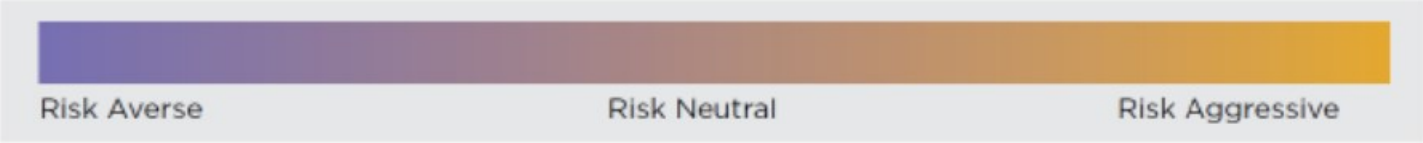
- Offers a comprehensive view of risk and enables more risk-aware decision making

Note: The framework provides a complete depiction of how to build a risk profile in an appendix

Source: COSO

Recognizes Importance of Culture

- Addresses the growing focus, attention and Importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within the broader context of overall core
- Depicts culture behavior within a risk spectrum



- Explores the possible effects of culture on decision making
- Explores the alignment of culture between individual and entity behavior

Source: COSO

Focuses on Decision Making

- Explores how enterprise risk management drives risk aware decision making
- Highlights how risk awareness optimizes and aligns decisions impacting performance
- Explores how risk aware decisions affect the risk profile

Source: COSO

Introduces Principles

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication, & Reporting

18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Source: COSO 2017 Executive Summary

1. Governance and Culture

Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.

Source: COSO 2017 Executive Summary

2. Strategy & Objective Setting

ERM, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

Source: COSO 2017 Executive Summary

2. Strategy & Objective Setting

Risk appetite is the aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan. High risk appetite vs lesser risk appetite - examples

Source: COSO 2017 Executive Summary

3. Performance

Risks that may impact the achievement of strategy and business objectives need to be identified and assessed.

Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

Source: COSO 2017 Executive Summary

4. Review & Revision

By reviewing entity performance, an organization can consider how well the ERM components are functioning over time and in light of substantial changes, and what revisions are needed.

Source: COSO 2017 Executive Summary

5. Information, Communications, & Reporting

ERM requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Source: COSO 2017 Executive Summary

Looking Into the Future

- Dealing with the proliferation of data:
  - More data becomes available
  - Speed at which new data can be analyzed increases
  - ERM will need to adapt
  - Data will come from both inside and outside the entity, and it will be structured in new ways
  - Artificial intelligence: Advanced analytics and data visualization tools will evolve and be very helpful in understanding risk and its impact, both positive and negative

Looking Into the Future

- We have entered the era of automated processes and artificial intelligence.
- Important for ERM practices to consider the impact of these and future technologies, and leverage their capabilities.
- Previously unrecognizable relationships, trends and patterns can be uncovered, providing a rich source of information critical to managing risk.

Looking Into the Future

- Managing the cost of risk management
  - Frequent concern expressed by many executives is the cost of risk management, compliance processes, and control activities in comparison to the value gained
  - As ERM practices evolve, it will become important that activities spanning risk, compliance, control, and even governance be efficiently coordinated to provide maximum benefit to the organization.

Looking Into the Future

- Building stronger credit unions
  - Credit unions will become better at integrating ERM with strategy and performance, an opportunity to strengthen resilience will present itself.
  - Knowing the risks that will have the greatest impact on the entity
  - Credit unions can use ERM to help put in place capabilities that allow them to act early, opening up new opportunities.
    - Indirect
    - High risk lending
    - Commercial loans

Elements of ERM

- Aligning risk appetite with strategies (examples)
  - Product lines (i.e., commercial lending and core business services)
  - Distribution channels (Internet, branch)
  - Product origination points (internal vs. external)
  - Product strategies (i.e., underwriting guidelines for loans, risk-based pricing for loans, relationship-based pricing for commercial relationships)

Enhancing Rigor of Risk-Response Decision

- Management should analyze risk of new products & processes, making decision based on risk-return
- High LTV indirect loans (considered higher risk) should be offset by significantly higher interest rates, capital position, and ability to manage servicing and collections
- Decision is made to grant (MBL) business loans (higher risk), but management will not lend to lending limit; instead, it sets a more conservative limit until it understands risks and is experienced in new line of business

Reducing Frequency & Severity of Operational Surprises & Losses

- Where are losses incurred?
  - Commercial lending
  - Real estate lending
  - Member check fraud
  - Internal fraud
  - Indirect loans
  - Fraudulent loans

- By studying risks related to operations, losses can be minimized
- Seek multiple experts and monitor tightly

Elements of ERM

- Proactively seizing on opportunities presented.
  - Example: mergers and acquisitions in the current market

Key Players for ERM Implementation

- Board of directors and executive team have overall responsibility for ensuring risks are identified and managed
- Management team is responsible for executing ERM
  - Identifying risks and managing them
- ERM requires everyone in an organization to participate to ensure successful enterprise-wide risk management

Components of ERM

Internal Environment

- Encompasses organization's tone
- Sets basis for how risk is viewed
- Addressed by
  - Risk management philosophy and risk appetite
  - Integrity and ethical values
  - Environment in which they operate

Internal Environment: Example

- Management has adopted an ERM strategy which is reflected in its corporate governance model; risk management activities are supported
- Management is risk-adverse and therefore has adopted conservative lending strategies and seeks A and B paper only
- MBLs are underwritten by credit group; borrower needs are the lender's responsibility
- Management leads by example and implemented an ethics policy each employee is required to abide by

Example of Risk Management Structure in a Large Credit Union

Objective Setting

- Must exist before management can identify potential events affecting its achievement
- ERM ensures management has a process in place to set objectives
  - Growth, liquidity, yield, margins, losses, costs
- ERM ensures objectives are inline with entity's mission and consistent with its risk appetite (capital, net income, and ability to monitor and understand)

Objective Setting: Example

- A credit union decides to enter into indirect auto lending and sets conservative objectives
  - Limits maximum LTVs based on credit scores (max 110% and only “A” borrowers)
  - Collateral risk and 72 – 84 month loans (higher losses per charged off loan)
  - Implements risk-based pricing (reflective of true risk or market competition)
  - Gains an understanding of the process prior to making the decision to get into the line of business
  - Hires experienced individuals to monitor the program
  - Policies and procedures are documented
  - Related risks are understood, analyzed, tested, and monitored
  - Liquidity, yield, and net compared to range of potential losses

Event Identification

- Internal and external events can affect achievement of objectives
  - Unemployment
  - Consumer price index, consumer confidence
  - Collateral value indexes (relevant)
- Events must be identified and distinguished between risk and opportunities
- Opportunities are channeled back to management's strategy or objective setting

Event Identification: Examples

- Internal events
  - New products, new systems, new delivery methods
- External events
  - Economy, accounting changes, regulatory changes, merger possibilities

Event Identification: Examples of External Events

- NCUA supervisory priorities for 2019
  - Bank Secrecy Act compliance (compliance risk)
  - Concentrations of credit (credit risk)
  - Consumer compliance (compliance risk)
    - HMDA, Regulation B, Military Lending Act
  - Current Expected Credit Losses/CECL (credit risk)
  - Information systems and assurance (transaction/strategic/reputation/compliance risks)
  - Liquidity and interest rate risks

Risk Assessment

- Risks should be analyzed considering likelihood (probability) and impact
- Analysis should be basis for determining how risk should be managed
- Risks should be analyzed on an inherent, controls and residual basis
- Frequency of risk evaluations is typically limited in credit unions

Types of Risk Assessments

- IT/GLBA
- Internal audit
- BSA/OFAC
- ACH
- Compliance (compliance management system)

Risk Response

- Management shall determine how to respond to risk
- Actions should be developed to align risks with risk tolerances and risk appetite - monitoring validates
- Relevant current risks
  - Rising real estate prices
  - Indirect loan losses; collateral value
  - Data breach

Information & Communication

- Relevant information should be identified, captured, and communicated
- Should be in a form and timeframe in order for people to carry out their responsibilities

Monitoring

- Entirety of ERM should be monitored and modified as necessary
- Accomplished through ongoing Board and ERM function (if any), plus management activities and separate evaluations

Monitor Limitations, Test Controls, and Report Test Results

- Determine test procedures
- Develop test plans
- Document tests and report results

Benefits of ERM

- Helps an organization manage risks to protect and enhance value by:
  - Focusing on establishing sustainable competitive advantage (loan rates, saving rates, fees)
  - Optimizes cost of managing risk
  - Helps management improve business performance
  - Sustainable member value
  - Reduce severity of economic swings (like now)
  - Forces an evaluation of products in comparison to capital
  - Makes a good argument for capital alternatives

Benefits of ERM

- Spending financial resources on the right initiatives
- Managing risk, responding early, and monitoring losses

Conclusion

Successful implementation of ERM will provide your Directors and executive management the ability to successfully manage risk and protect your members' value proposition, while ensuring the ability to sustain your credit union's business model.

Questions?

DoerenMayhew
CPAs AND ADVISORS

Thank you

Robin D. Hoag, CPA, CGMA, CMC
Shareholder
Cell: (248) 709-1270
Email: hoag@doeren.com

Joseph A. Zito, CPA, MBA
Shareholder
Office: (248) 244-3068
Cell (586) 291-4311
Email: zito@doeren.com

DoerenMayhew
CPAs AND ADVISORS