ENTERPRISE RISK MANAGEMENT, IN PERSPECTIVE

ACUIA Regional Meeting
October 8, 2020

Lisa B. Berry, CRCM

www.lisa.berry@warrenaverett.com

205.368.5689

Warren Averett
CPAs AND ADVISORS

Agenda

- Enterprise Risk Management (ERM) Overview
- Foundations of an ERM program
- Industry Guidance
- Regulatory Requirements
- Enterprise Risk Management Committee
- Risk Assessment
- Risk Management, Monitoring and Reporting
- ERM Benefits for ALL Credit Unions

ENTERPRISE RISK MANAGEMENT (ERM) OVERVIEW

Warren Averett
CPAs AND ADVISORS

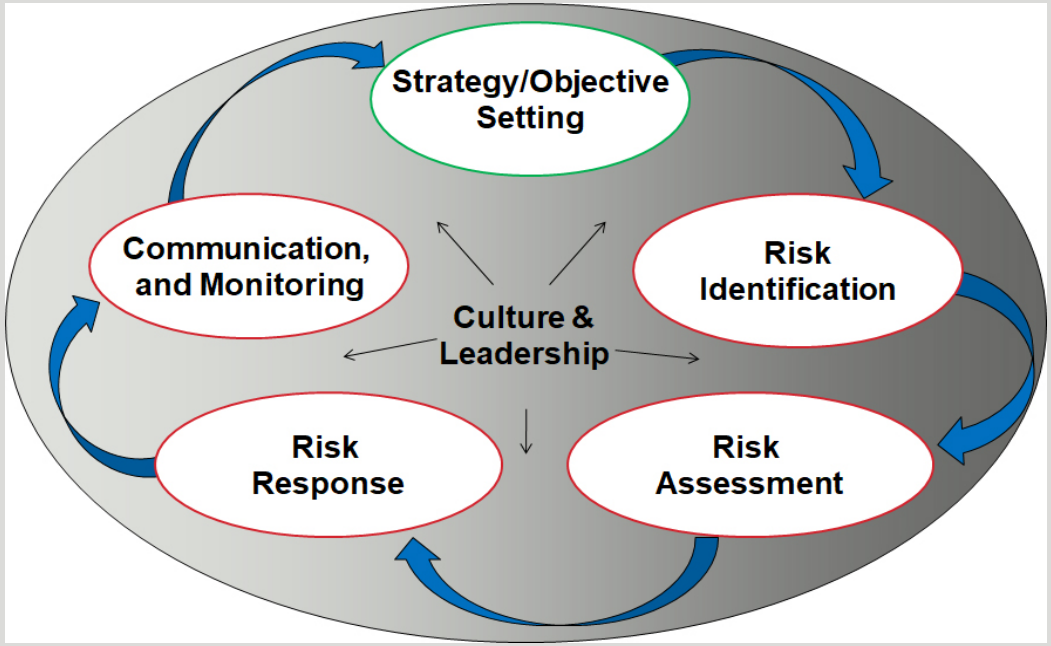
ERM DEFINED

"Enterprise risk management (ERM) is 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."

The Committee of Sponsoring Organizations (COSO) of the Treadway Commission, (Sept. 2004)

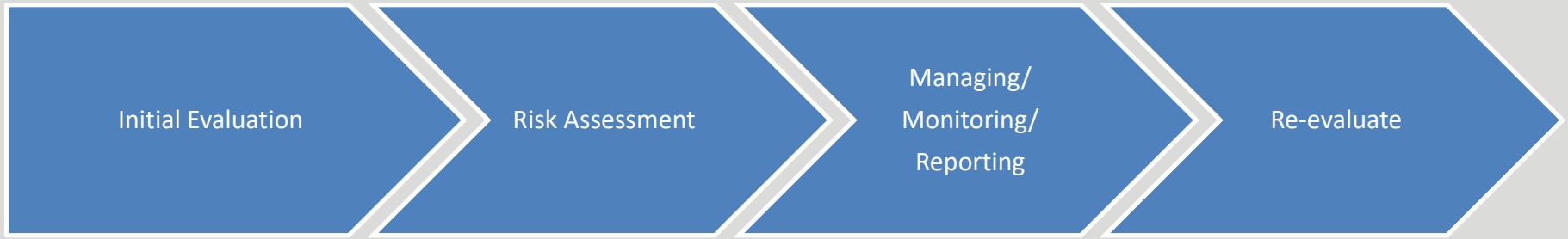
WHAT IS ERM?

- ERM is an ongoing process that must inform business strategy
- It is a collaborative process to identify, manage and monitor organizational internal and external risks and opportunities, to ensure achievement of the credit union's strategic goals and continued financial resilience.



FOUNDATIONS OF AN ERM PROGRAM

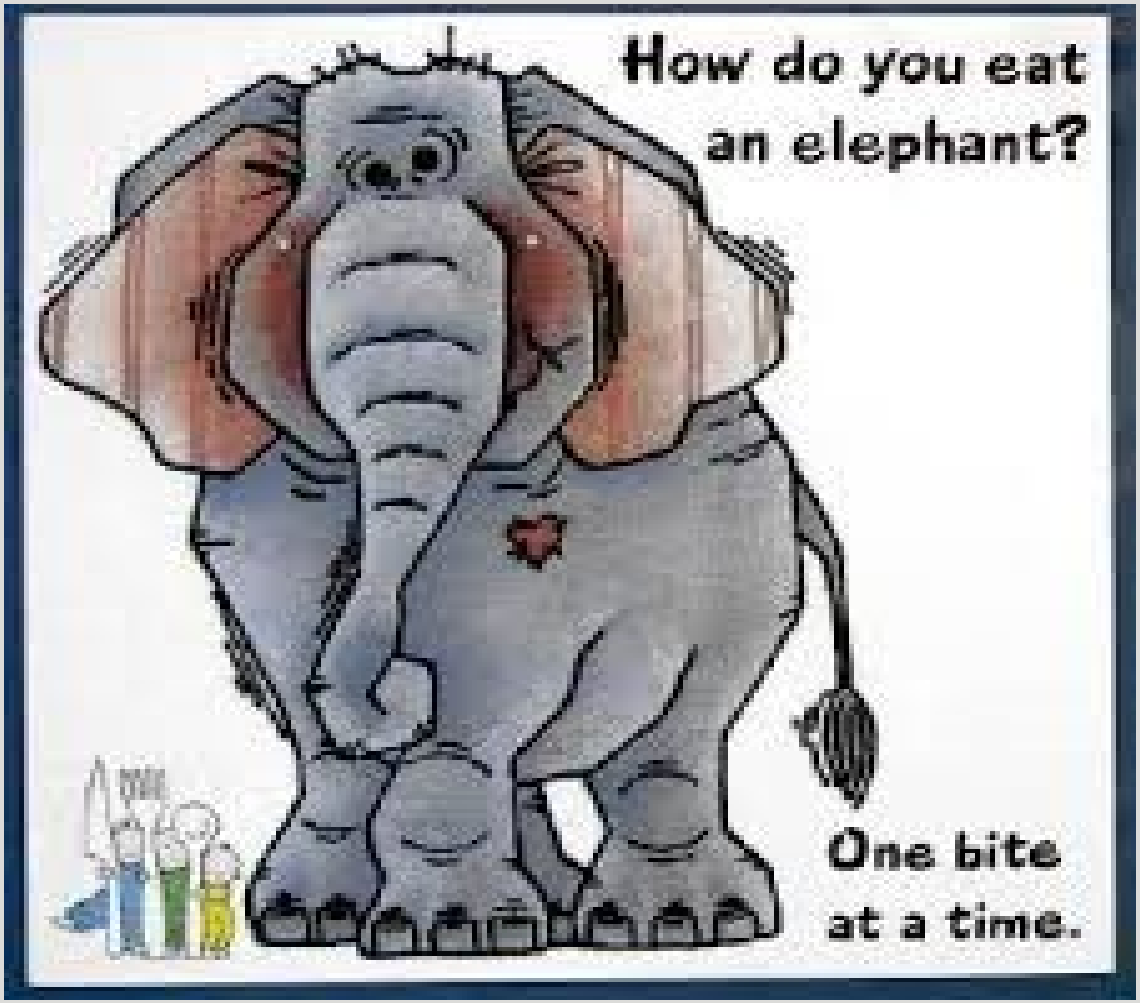
STEPS IN THE PROCESS



Warren Averett
CPAs AND ADVISORS

ERM MUST-HAVES

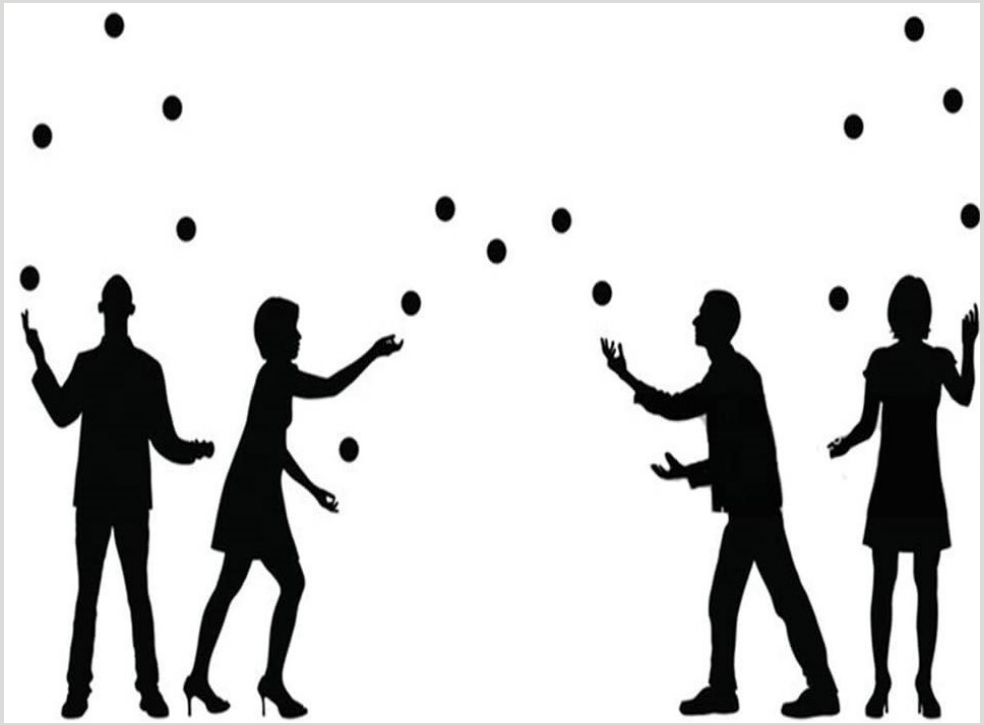
1. **Board and Senior Management Leadership and Oversight**
2. Appointment of a leader empowered to drive the initiative
3. Establish a Risk Committee and Working Groups
4. Conduct an Enterprise-wide Risk Assessment
5. Create and maintain an inventory from the risk assessment with the risks tiered
6. Identify gaps
7. Assign Ownership
8. Develop reporting
9. Continuous monitoring and action plans with follow up
10. Re-educate and reevaluate



Warren Averett
CPAs AND ADVISORS

KEY IMPLEMENTATION FACTORS

1. Begins with the **Tone at the Top**
2. Establishing an ERM organization
3. Performing risk assessments
4. Determining overall risk appetite
5. Identifying risk responses
6. Communication of risk results
7. Monitoring
8. Oversight & periodic review by management



Warren Averett
CPAs AND ADVISORS

INDUSTRY GUIDANCE

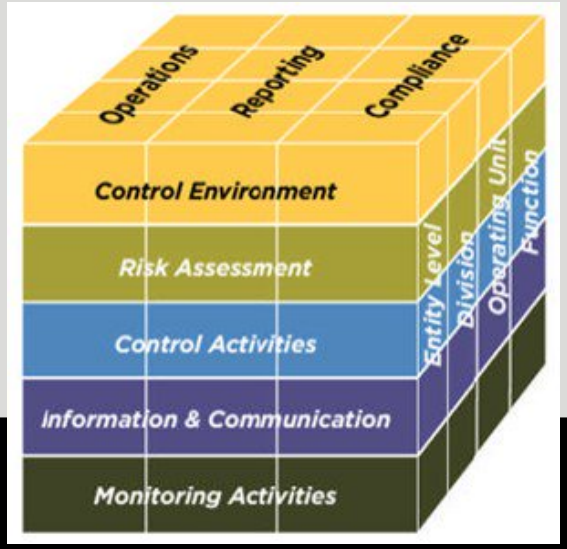
INDUSTRY GUIDANCE

While Section 704.21 does not require the use of a particular ERM framework, the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework is widely recognized in the financial services industry.

COSO (Committee of Sponsoring Organizations of the Treadway Commission)

- Adopted by many financial institutions
- Includes key components that could help financial institutions derive business value while meeting compliance requirements.
- Structured around eight key components and four key objectives of business or strategic plans, operations, reporting and compliance.

*Each credit union should choose an ERM framework that is appropriate to its **size** and **complexity.***



COSO PILLARS

Warren Averett
CPAs AND ADVISORS

THE FRAMEWORK ITSELF IS A SET OF PRINCIPLES ORGANIZED INTO FIVE INTERRELATED COMPONENTS:

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.
2. **Strategy and Objective-Setting:** Enterprise risk management, 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.
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.
4. **Review and Revision:** By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting:** Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down and across the organization.

COMPONENTS & PRINCIPLES

GOVERNANCE AND CULTURE

1. **Exercises Board Risk Oversight –** The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes Operating Structures –** The organization establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines Desired Culture –** The organization defines the desired behaviors that characterize the entity's desired culture.
4. **Demonstrates Commitment to Core Values –** The organization demonstrates a commitment to the entity's core values.
5. **Attracts, Develops, and Retains Capable Individuals –** The organization is committed to building human capital in alignment with the strategy and business objectives.

COMPONENTS & PRINCIPLES

STRATEGY AND OBJECTIVE-SETTING

6. **Analyzes Business Context –** The organization considers potential effects of business context on risk profile.
7. **Defines Risk Appetite –** The organization defines risk appetite in the context of creating, preserving, and realizing value.
8. **Evaluates Alternative Strategies –** The organization evaluates alternative strategies and potential impact on risk profile.
9. **Formulates Business Objectives –** The organization considers risk while establishing the business objectives at various levels that align and support strategy.

COMPONENTS & PRINCIPLES

PERFORMANCE

10. **Identifies Risk –** The organization identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses Severity of Risk –** The organization assesses the severity of risk.
12. **Prioritizes Risks –** The organization prioritizes risks as a basis for selecting responses to risks.
13. **Implements Risk Responses –** The organization identifies and selects risk responses.

COMPONENTS & PRINCIPLES

REVIEW AND REVISION

14. **Develops Portfolio View –** The organization develops and evaluates a portfolio view of risk.
15. **Assesses Substantial Change –** The organization identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews Risk and Performance –** The organization reviews entity performance and considers risk.

COMPONENTS & PRINCIPLES

INFORMATION, CONFIRMATION AND REVIEW

14. **Pursues Improvement in Enterprise Risk Management –** The organization pursues improvement of enterprise risk management.
15. **Leverages Information Systems –** The organization leverages the entity's information and technology systems to support enterprise risk management.
16. **Communicates Risk Information –** The organization uses communication channels to support enterprise risk management.
17. **Reports on Risk, Culture, and Performance –** The organization reports on risk, culture, and performance at multiple levels and across the entity.

REGULATORY REQUIREMENTS

IMPLEMENTING 704.21

"Sound risk management is an integral part of running a [corporate] credit union. A well designed ERM process can help a [corporate] by providing a framework within which the board of directors and senior management can determine:

- Where the [corporate]'s risk exposures lie;
- The amount of risk the [corporate] has in each exposure;
- The maximum levels of risk it is willing to accept;
- How the risk exposures are changing; and
- The appropriate risk controls to limit overall risk to targeted levels.

ERM will enable [corporates] to move away from the "silo" approach of risk management and move towards the "holistic" view of enterprise wide risks. A [corporate] must be able to measure and understand not only all of the individual risks associated with its various business components but also how the risks interact dynamically."

NCUA's July 2013 "Implementing 704.21 – Enterprise Risk Management"

IMPLEMENTING 704.21

Section 704.21 of the NCUA's Rules and Regulations **requires** [**corporate**] credit unions to develop and follow an **Enterprise Risk Management policy.**

Note: *704.21 addresses the* ***requirements*** *for corporate credit unions and for that purpose we have included corporate in brackets. However, for natural person credit unions, simply remove the word [corporate] and consider how this will benefit your organization. Enterprise Risk Management works for everyone.*

Let's put ERM in perspective for all of us.

ERM POLICY

The rule does not specifically define the components of an ERM policy. However, critical elements for developing a sound ERM program should include:

- Understanding the risk appetite,
- Setting the tone for risk governance
- Establishing a compliant risk culture across the organization.

ERM POLICY & PROGRAMS

Financial institutions' ERM policies and programs generally include:

- **Creating** a standardized, enterprise-wide risk framework
- **Setting** risk objectives and ensuring that they align to the credit union's objectives, risk appetite and culture.
- **Ensuring** management and oversight of identified risks remains independent of business lines or specific areas of operations.
- **Using** internal stress testing strategies, systems and procedures. This may include defining internal model governance groups responsible for the independent review and validation of models.
- **Incorporating** liquidity management into the ERM process, specifically understanding liquidity pressures through the liquid coverage ratio, net stable funding ration and new liquidity reporting as well as including liquidity in stress tests and other financial models.
- **Capital management** to more effectively evaluate the capital required to absorb known losses, anticipated losses through modeling scenarios, as well as capital needed to absorb future unanticipated losses.

ENTERPRISE RISK MANAGEMENT COMMITTEE

SECTION 702.41

Section 704.21 of the NCUA's Rules and Regulations requires [corporate] credit unions to establish an **Enterprise Risk Management Committee (ERMC)** that is responsible for reviewing and overseeing the [corporate's] risk management practices.

The ERMC must **report on the committee's activities**, at least quarterly, to the board of directors.

The ERMC must **include at least one independent risk management expert** with sufficient experience in identifying, assessing, and managing risk exposures applicable to the [corporate].

The rule defines *independent* to mean that neither the expert, nor any immediate family member of the expert, is supervised by, or has any material business or professional relationships with; the chief executive officer (CEO) of the [corporate] credit union, or anyone supervised, directly or indirectly, by the CEO, and has been free of any such relationships for at least three years.

THE ENTERPRISE RISK MANAGEMENT COMMITTEE

It is critical that the ERM policy is appropriate for the ***size***, ***complexity*** and ***risk*** profile of the credit union. The ERMC will be involved in establishing the ERM Program according to the policy. ERM is an evolving discipline and a "one-size fits all" approach is not suitable for all credit unions.

The ERMC acts in an advisory capacity to the board of directors to ensure the board obtains comprehensive information on all if the credit union's risks **holistically**, and not in a siloed fashion. *For example*, before the credit union initiates new products or services, Information Technology should be consulted to ensure the systems are prepared to adequately process the new products. Compliance should be consulted to ensure the product or service is compliant with regulatory requirements. The ERMC should conduct its risk analysis and present its views <u>independent</u> of the earnings opportunities or pressures of the product or service. Evaluating the risks across the credit union allows the board to better define risks qualitatively and quantitatively to determine the credit union's ability to absorb losses through capital and retained earnings accumulations.

RISK ASSESSMENT

Key Questions

1. What are all the risks to our business strategy and operations (coverage)?
2. How much risk are we willing to take (risk appetite)?
3. How do we govern risk taking (culture, governance, and policies)?
4. How do we capture the information we need to manage these risks (risk data and infrastructure)?
5. How do we control the risks (control environment)?
6. How do we know the size of the various risks (measurement and evaluation)?
7. What are we doing about these risks (response)?
8. What possible scenarios could hurt us (stress testing)?
9. How are various risks interrelated (stress testing)?

RISK ASSESSMENT MATURITY CURVE

Ad Hoc

- No enterprise-wide risk assessment preformed
- Individual business units may be conducting their own risk assessments

Developing

- Annual enterprise-wide risk assessment is conducted.
- Common risk categories or definitions are used.
- Enterprise-wide risk ranking or risk profile is produced

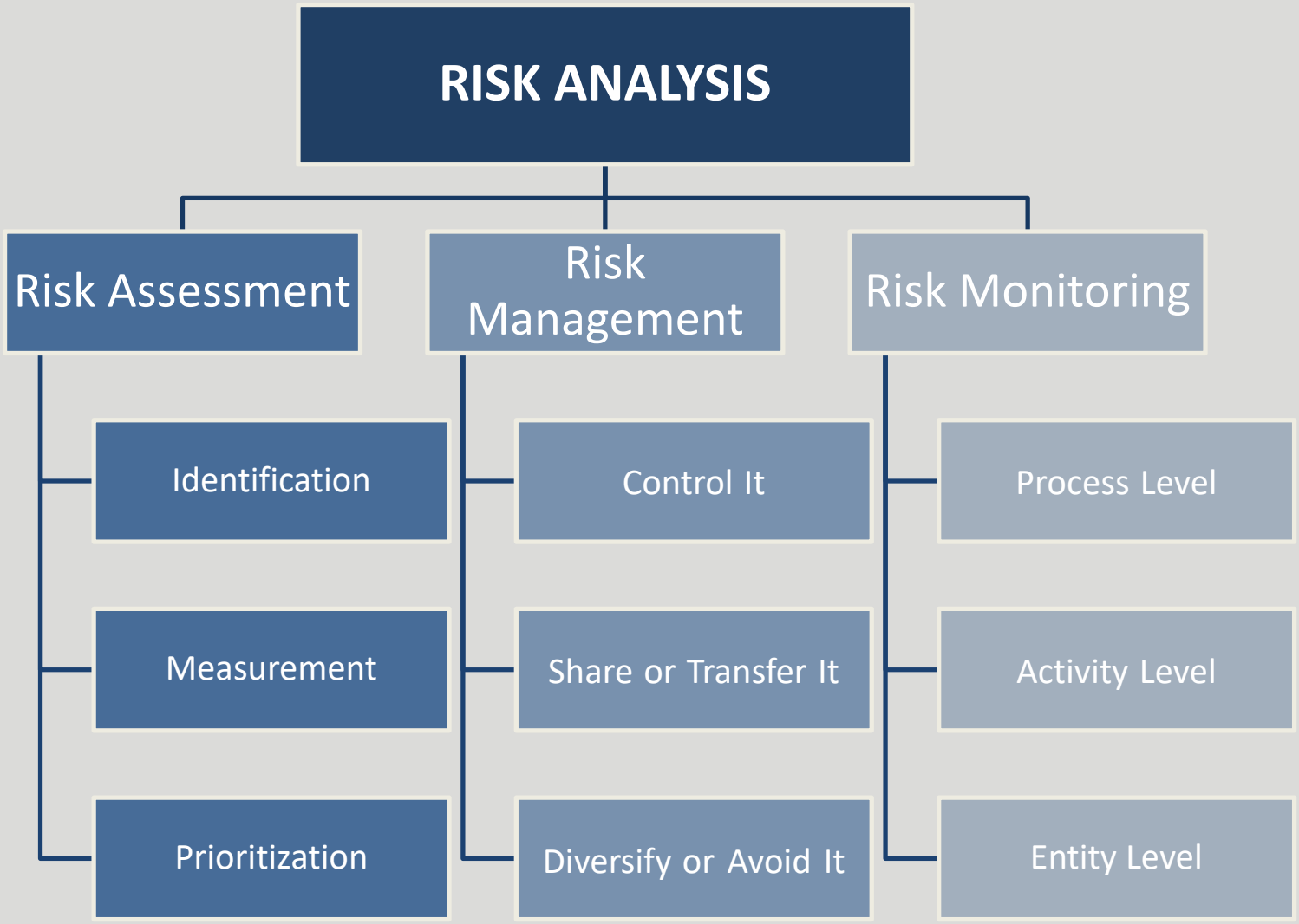
Enhanced

- Enterprise risk assessment updated on quarterly basis
- Management risk committee is in place, including business unit leaders
- Process includes identifying emerging issues or events
- Common risk assessment methodology established and used across the organization.

Leading Practice

- Risk owners conducts ongoing updating of reorganization's risks.
- Technology enabled monitoring of KRIs used to update.
- Real time risk profile or dashboard available to management
- Risk assessment process aligned with budgeting and the strategic planning process

Warren Averett
CPAs AND ADVISORS

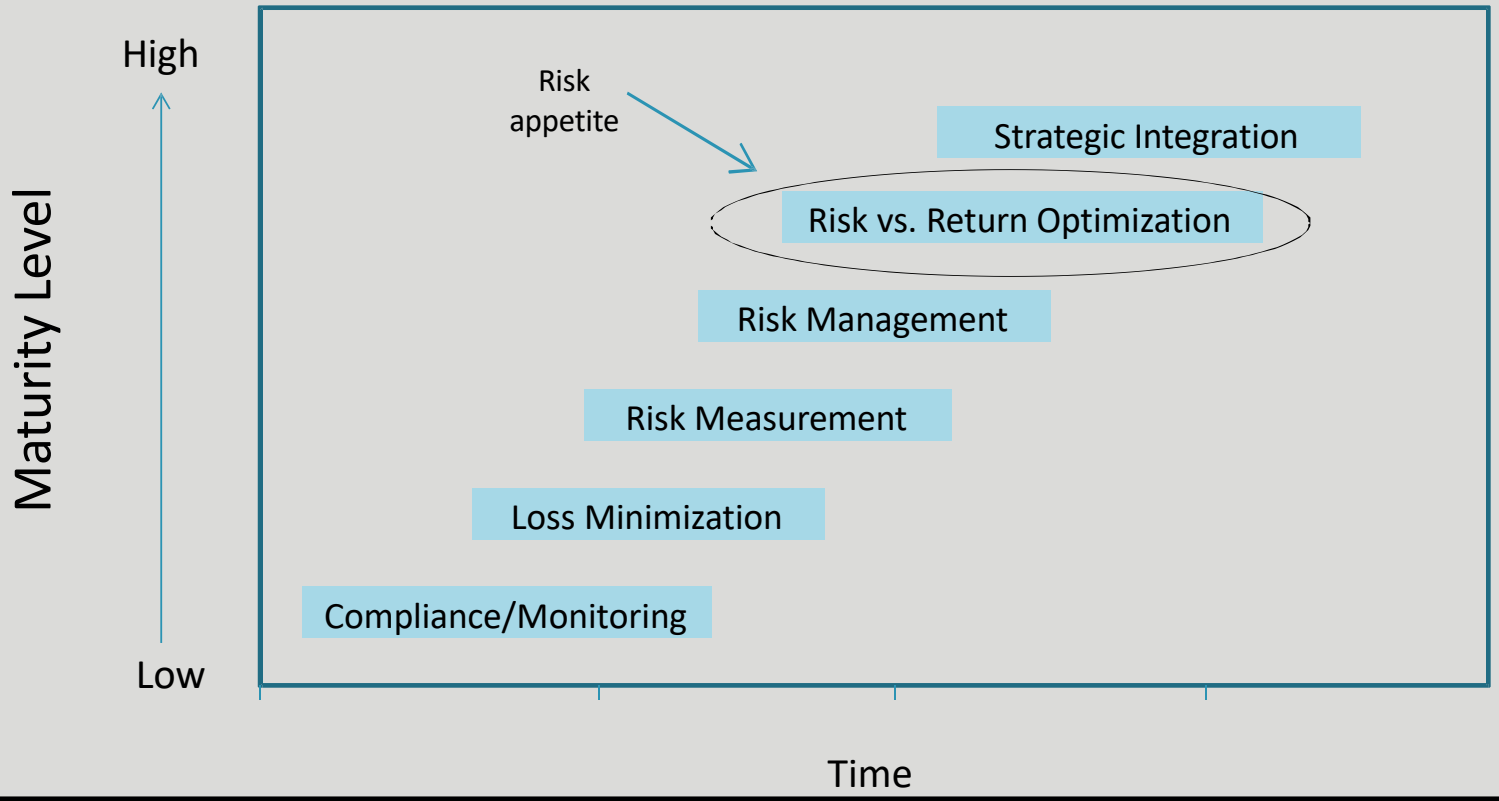


Source: Business Risk Assessment. 1998 – The Institute of Internal Auditors

ERM Strategy Gap Analysis

Core ERM Processes	Current State	Desired State	Key Actions	Timeframe to Implement	Responsible Person
a. Risk Culture					
b. ERM Framework and Program					
c. Communications					
d. Accountability					
e. Risk Assessment Process					
f. Reporting					
g. Risk Appetite Tolerances					
h. Core Competency					
i. Linkage to Compensation					
j. Linkage to Performance Measurement					
k. ERM Performance Measurement					
l. ERM Strategy					

STRATEGIC ERM



Warren Averett
CPAs AND ADVISORS

RISK PROFILE

Risk Category	Quantity of Risk (Low, Moderate, High)	Quality of Risk Management (Weak, Satisfactory, Strong)	Aggregate Level of Risk (Low, Moderate, High)	Direction of Risk (Increasing, Stable, Decreasing)
Credit				
Interest Rate				
Liquidity				
Price				
Operational				
Compliance				
Strategic				
Reputation				

NOTE: Risk assessments indicated in bold or italic type reflect a change since the last assessment.

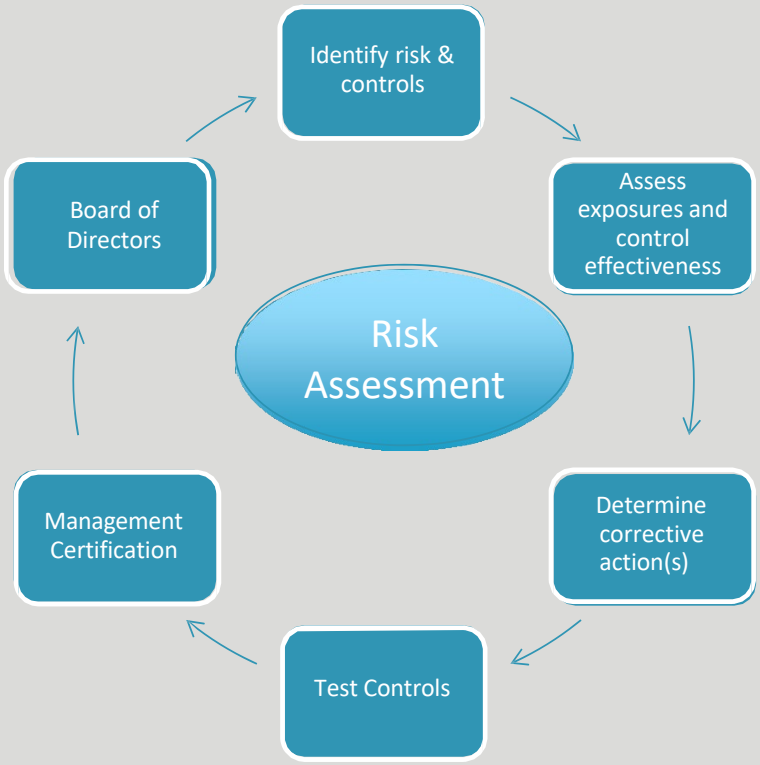
Risk Type	Description	Likelihood	Impact	Velocity	Readiness	Priority
Compliance/Legal/Regulatory		Medium	High	Slow		1
Credit		Low	High	Fast		1
Operational		High	Medium	Slow		1
Liquidity		Medium	Low	Fast		1
Market		Low	High	Fast		2
Financial		Low	Medium	Slow		3
Capital Adequacy		Medium	High	Medium		1
Reputational		Low	High	Fast		2

Warren Averett
CPAs AND ADVISORS

RISK ASSESSMENT CYCLE

Risk Assessments

- Should be practical, sustainable, and easy to understand
- Process should be done in a structured and disciplined way
- Should be standardized across the organization
- Should be customized to the size, complexity, and geographic area of your organization
- Should be a used in the decision-making and strategic planning process of your organization



Define Your Risk Appetite

Existing Risk Profile	The existing level and distribution of risks across risk categories (e.g. financial risk, market risk, operational risk, reputation risk, etc.
Risk Capacity	The Maximum risk a firm may bear and remain solvent
Risk Tolerance	Acceptable levels of variations an entity is willing to accept around specific objectives
Desired Level of Risk	What is the Desired risk / return level

Determination of Risk Appetite
(the amount of risk an entity is willing to accept in the pursuit of value)

WAYS TO DEFINE RISK

Quantitative	**Clearly defined measure Can be cascaded to business units For example, loss of capital or degree of volatility in earnings**
Qualitative	Not all risks can be accurately/credibly measured For example, risk of damage to reputation
Zero Tolerance	A subset which can be very clearly defined For example, loss of life or violation of laws

RISK MANAGEMENT PROCESS COMPONENTS

Key Components must include:

- Risk Identification
  - What are your key risks?
  - What level of risk is allowed by your risk appetite?
- Risk Measurement
  - Are risks defined?
  - Do you have models that measure key risks?
- Risk Control
  - Policies
  - Authorities and oversight
- Risk Monitoring/Reporting
  - KRIs and KPIs
  - Board and Management Self assessments

ERM BENEFITS FOR ALL CREDIT UNIONS

BENEFITS OF ENTERPRISE RISK MANAGEMENT

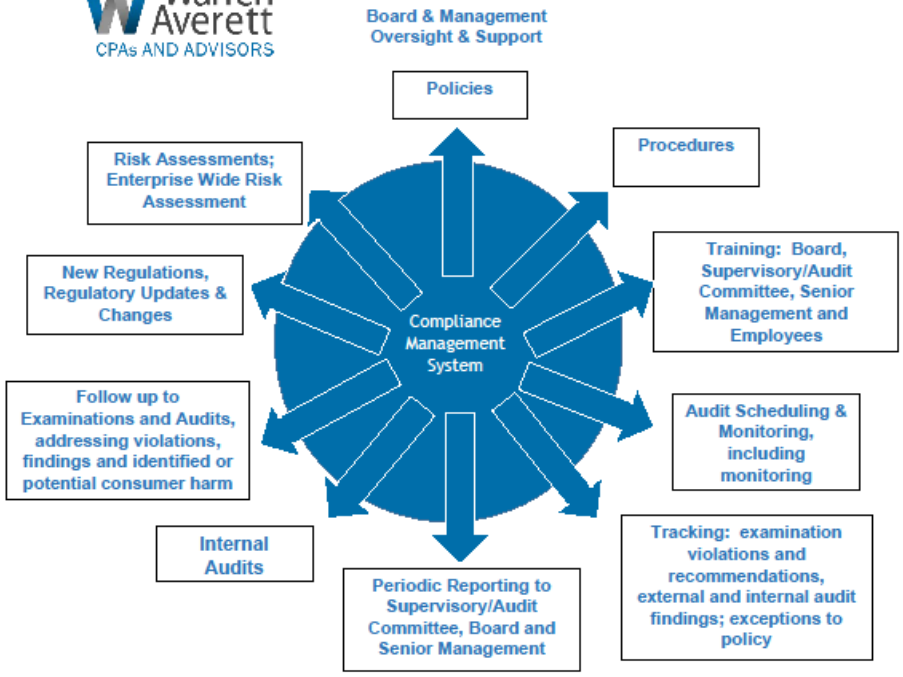
Sound risk management is an integral part of running any credit union. A well designed ERM process can help the credit union by providing a framework within which the board of directors and senior management can determine:

- Where the credit union's risk exposure lies
- The amount of risk the credit union has in each exposure
- The maximum levels of risk the credit union is willing to accept
- How the risk exposures are changing; and
- The appropriate risk controls to limit overall risk to targeted level

BENEFITS OF ENTERPRISE RISK MANAGEMENT

ERM programs have several key objectives, including:

- Identifying and evaluating the greatest risks to the credit union's strategic objectives.
- Developing a standardized organization-wide risk assessment process.
- Developing management plans for the most significant financial, operational, and strategic risks.
- Monitoring the effectiveness of operations and the status of any needed changes.
- Ensuring the credit union maintains compliance with all applicable laws and regulations without incurring excessive implementation and support costs.



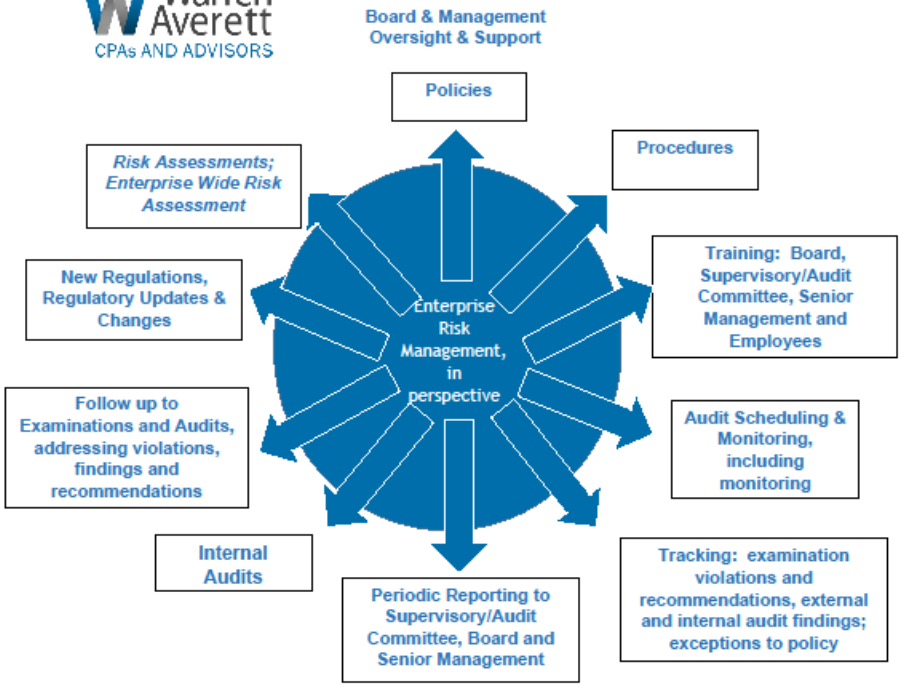
Lisa B. Berry, CRCM, CCBCO
Lisa.Berry@warrenaverett.com
205.769.3388

Ann B. Carver, CPA
Ann.Carver@warrenaverett.com
850.542.4111

Niki Dean, CPA
Niki.Dean@warrenaverett.com
850.542.4115

Warren Averett
CPAs AND ADVISORS

Warren Averett
CPAs AND ADVISORS



Lisa B. Berry, CRCM, CCBCO
Lisa.Berry@warrenaverett.com
205.769.3388

Ann B. Carver, CPA
Ann.Carver@warrenaverett.com
850.542.4111

Niki Dean, CPA
Niki.Dean@warrenaverett.com
850.542.4115

Warren Averett
CPAs AND ADVISORS

RESOURCES

- Credit Union Act https://www.ncua.gov/Legal/Documents/fcu_act.pdf
- https://www.ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/update-ncuas-2020-supervisory-priorities
- NCUA (National Credit Union Administration) https://www.ncua.gov/regulation-supervision/Pages/default.aspx
- Credit Union National Association www.cuna.org
- https://www.ncua.gov/regulation-supervision/corporate-credit-union-guidance-letters/implementing-section-70421-enterprise-risk-management
- https://www.fdicoig.gov/report-release/fdic's-implementation-enterprise-risk-management
- FDIC Risk-Based Assessment System – Financial Institution Letters (FILs) https://www.fdic.gov/deposit/insurance/risk/FILS.html

- https://www.occ.gov/publications-and-resources/publications/banker-education/files/pub-risk-appetite-statement.pdf
- OCC Bulletin 2015-48 Updated Guidance on Risk Assessment System (https://www.occ.gov/news-issuances/bulletins/2015/bulletin-2015-48.html#)
- OCC Comptroller's Handbook: Community Bank Supervision https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/pub-ch-ep-cbs.pdf
- COSO (The Committee of Sponsoring Organizations of the Treadway Commission) www.coso.org

CPAs AND ADVISORS

LET’S THRIVE TOGETHER

WARREN AVERETT

RISK MANAGEMENT & COMPLIANCE SERVICES FOR FINANCIAL INSTITUTIONS

Warren Averett has a deep understanding of credit union operations and risk management gained from performing many external and internal audits for financial institutions of differing sizes.

Our firm's extensive knowledge of the Sarbanes-Oxley (SOX) services pursuant to the COSO framework allows us to create an efficient and effective Enterprise Risk Management program.

Warren Averett
CPAs AND ADVISORS

WARREN AVERETT ERM ENGAGEMENTS

- Follow the revised ERM COSO framework (June 2017)
- Allow for risk to be aggregated across multiple risk in an enterprise-wide manner (historically risk has been managed in a siloed fashion)
- Increase risk awareness throughout an organization allowing for more informed operational and strategic decision-making

WARREN AVERETT

RISK MANAGEMENT & COMPLIANCE SERVICES WE PROVIDE FOR FINANCIAL INSTITUTIONS:

- Risk Assessments
- Enterprise Risk Management Consulting and Training
- ACH Reviews
- Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Reviews
- Regulatory compliance services including but not limited to:
    - Compliance Management System Review
    - Loan Compliance Reviews
    - Deposit Compliance Reviews
    - Fair Lending
    - HMDA scrub services