Creating Value through ERM and Internal Audit

Scott Hood

ROCHDALE + PARAGON

ACUIA
Association of Credit Union Internal Auditors

28th Annual Conference

June 2018

Agenda

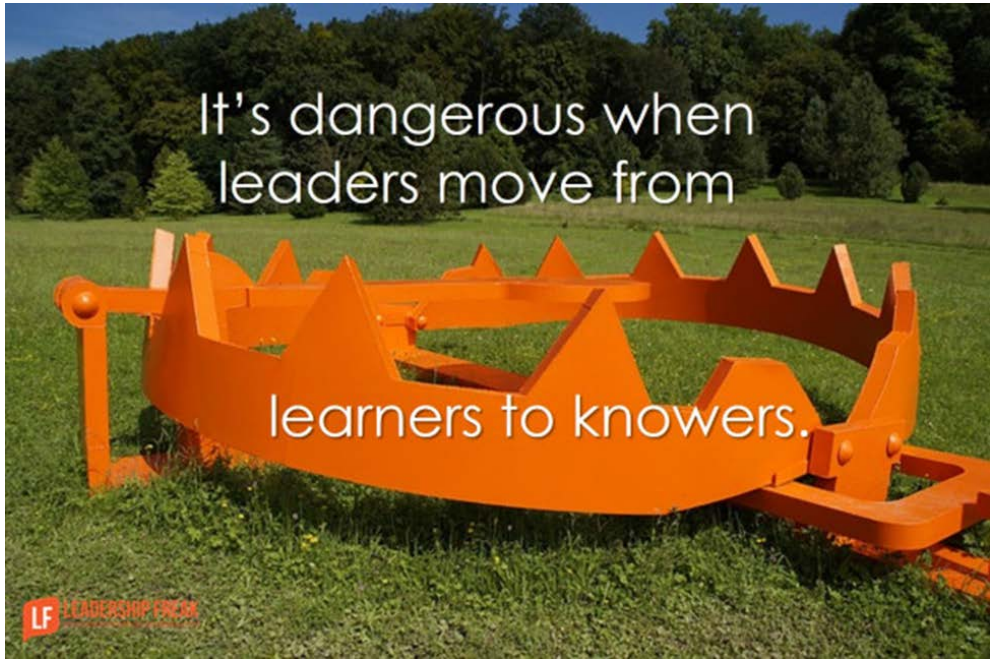
- Overview of ERM
- Risk Appetite Concepts
- ERM and Internal Audit

COSO ERM Definition

"… the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."

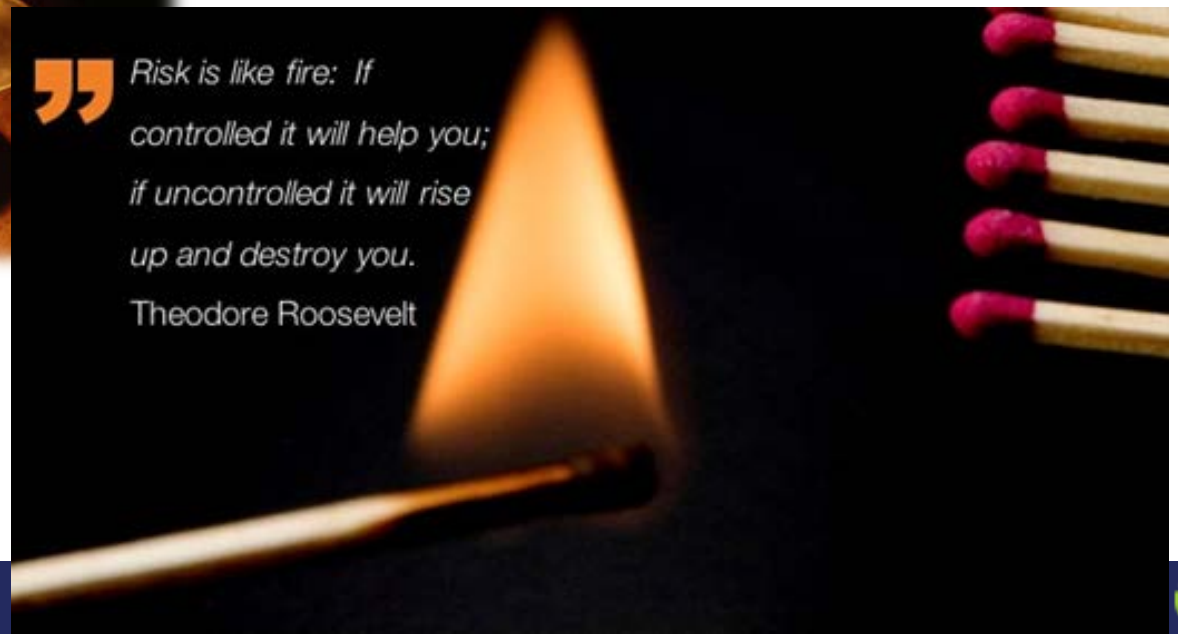
What is ERM?

- Improved organizational decision making through unobstructed knowledge, yielding better organizational performance

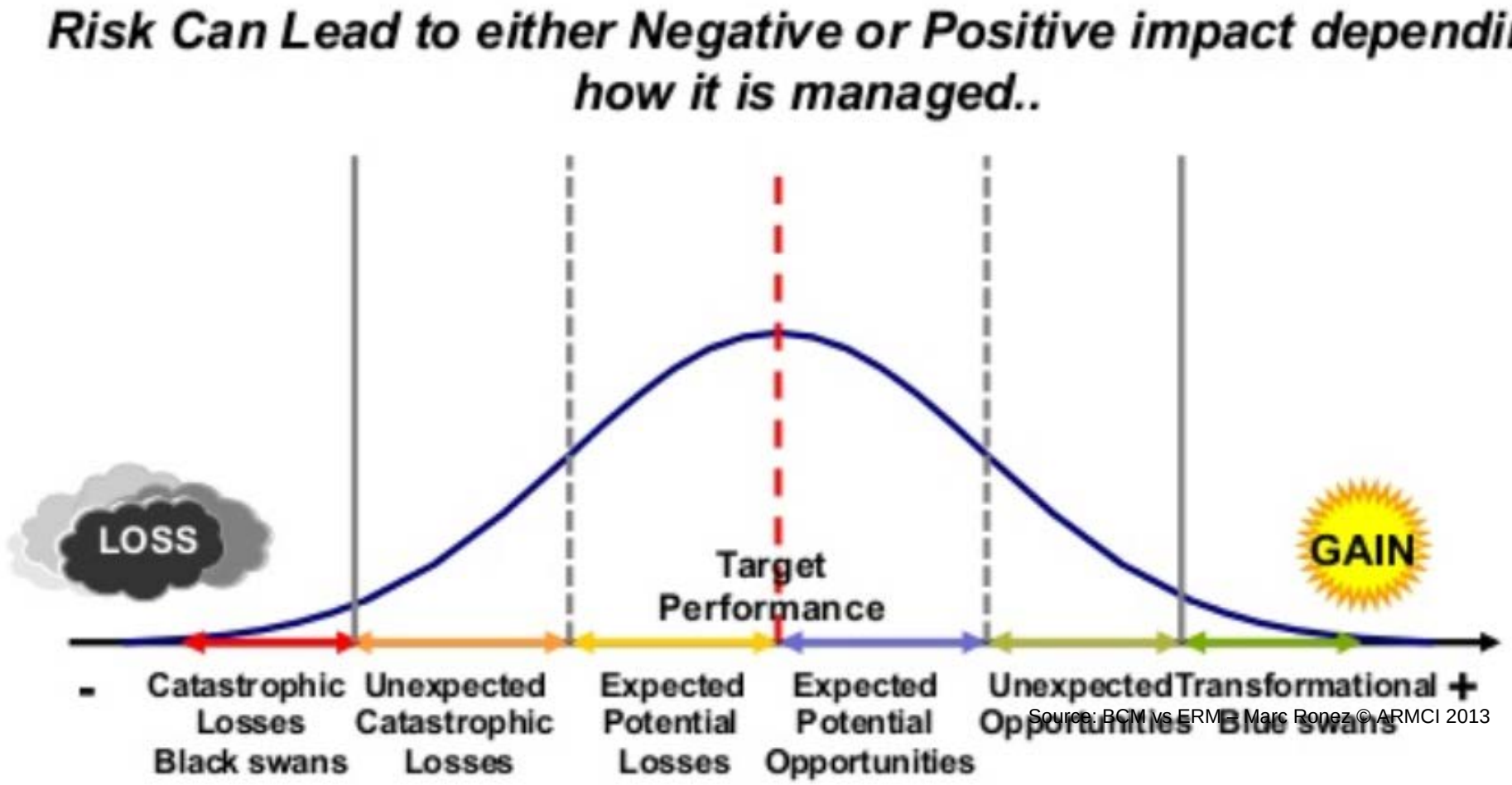


What is Risk?

- Possibility of suffering harm or loss
- Potential of losing something of value, weighed against the potential of gaining something of value
- Uncertainty



Loss vs Gain



Source: BCM vs ERM - Marc Ronez © ARMCI 2013

NCUA View of ERM

- Supervisory Letter issued to all Field Staff on November 7, 2013:
  - Discussed how NCUA views ERM as one framework for managing risk and NCUA's supervisory expectations with regard to credit unions' risk management programs
  - Emphasized that natural person credit unions are not required to implement a formal ERM framework, but are expected to have sound processes sufficient to manage the risk associated with their business model and strategies

NCUA Key Points on ERM

- Risk-optimization, not elimination
- Aligns risk with strategic objectives
- Takes enterprise-wide view of risks
- Reduces silos and fosters communication
- Board of directors engaged in ERM
- Encourages organizations to:
  - Take a broad look at all risk factors
  - Understand the interrelationships among those factors
  - Define an acceptable level of risk
  - Continuously monitor functional areas to ensure that the defined risk threshold is maintained

Red Flags for Examiners

1. Lack of commitment to risk management
2. Disengaged leadership
3. Concentrated organizational power or control
4. Inconsistent or weak process for complexity or risk level
5. Failure to adhere to policies and procedures
6. Appetite “creep” (Don’t rationalize – make the tough decision)
7. “Silver Bullets” and “Shiny Objects” (Don’t rationalize – make the tough decision)
8. Disproportionate yields = unidentified risk
9. A state of denial (It is not hard to know what is right, the hard thing is doing the right thing.)
10. Misaligned incentives (poorly designed pay and incentive plans)

Five ERM Interrelated Components

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

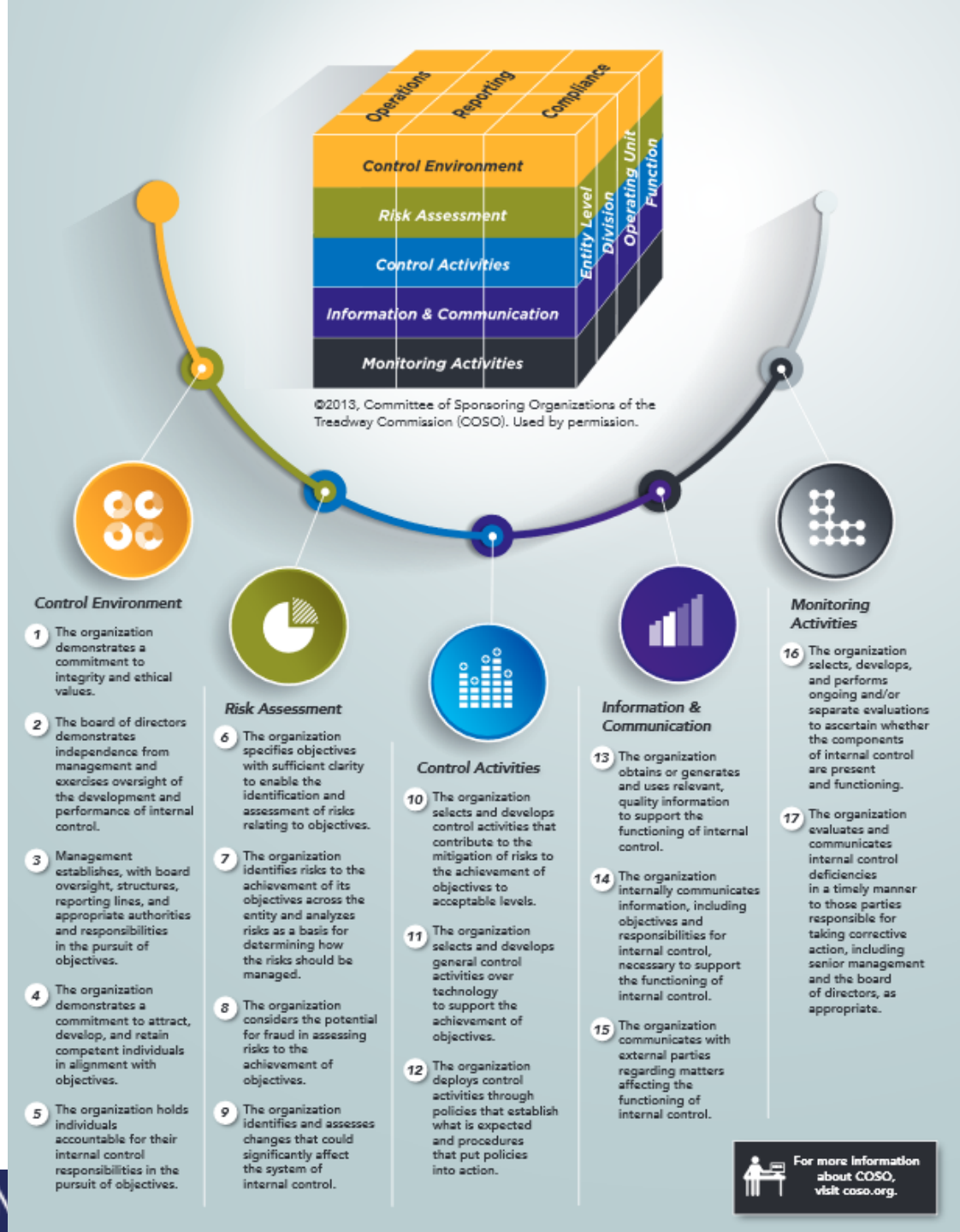
15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues improvement in Enterprise Risk Management

Information, Communication, & Reporting

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

ERM is Closely Linked to Internal Audit and Control

- Greater confidence regarding the achievement of entity objectives
- Greater confidence in the organization's ability to identify, analyze, and respond to risk and changes in the business and operating environments



What is Risk Appetite?

"The types and amount of risk, on a broad level, an organization is willing to take in pursuit of value"

- Almost always involves risk-return trade-offs
- A tool to use in managing our approach to achieving goals and strategies

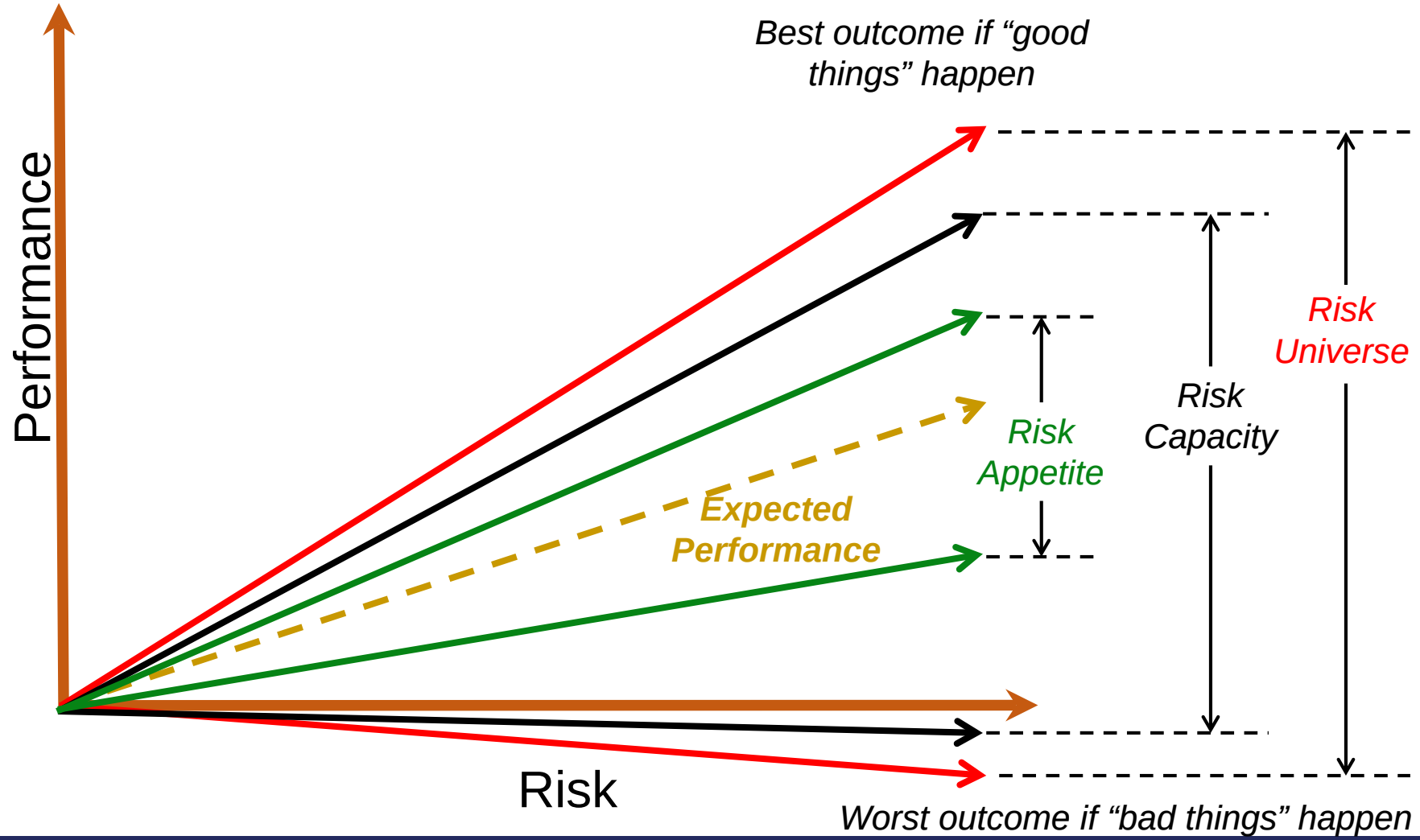
Considerations Affecting Risk Appetite

- Current level of risk across the organization
- Capacity of organization to assume risk
- Level of variation in performance the organization is willing to accept
- Attitudes towards growth, risk and return
- Other factors such as speed of changes in the organization’s environment

Why understand risk appetite?

- Integral link between enterprise risk management (ERM) and strategic planning
- Represents an acceptable path to reach our goals
- Helps guide strategic objectives, resource allocation, alignment and other key decisions
- A tool to improve organizational performance

Think of the Budgeting Process



Risk Appetite in a Strategic Planning Context

Risk Appetite: Are we willing to follow the path to our future?

If not:

a) Revisit where we want to be, or

b) Challenge the ways we do things

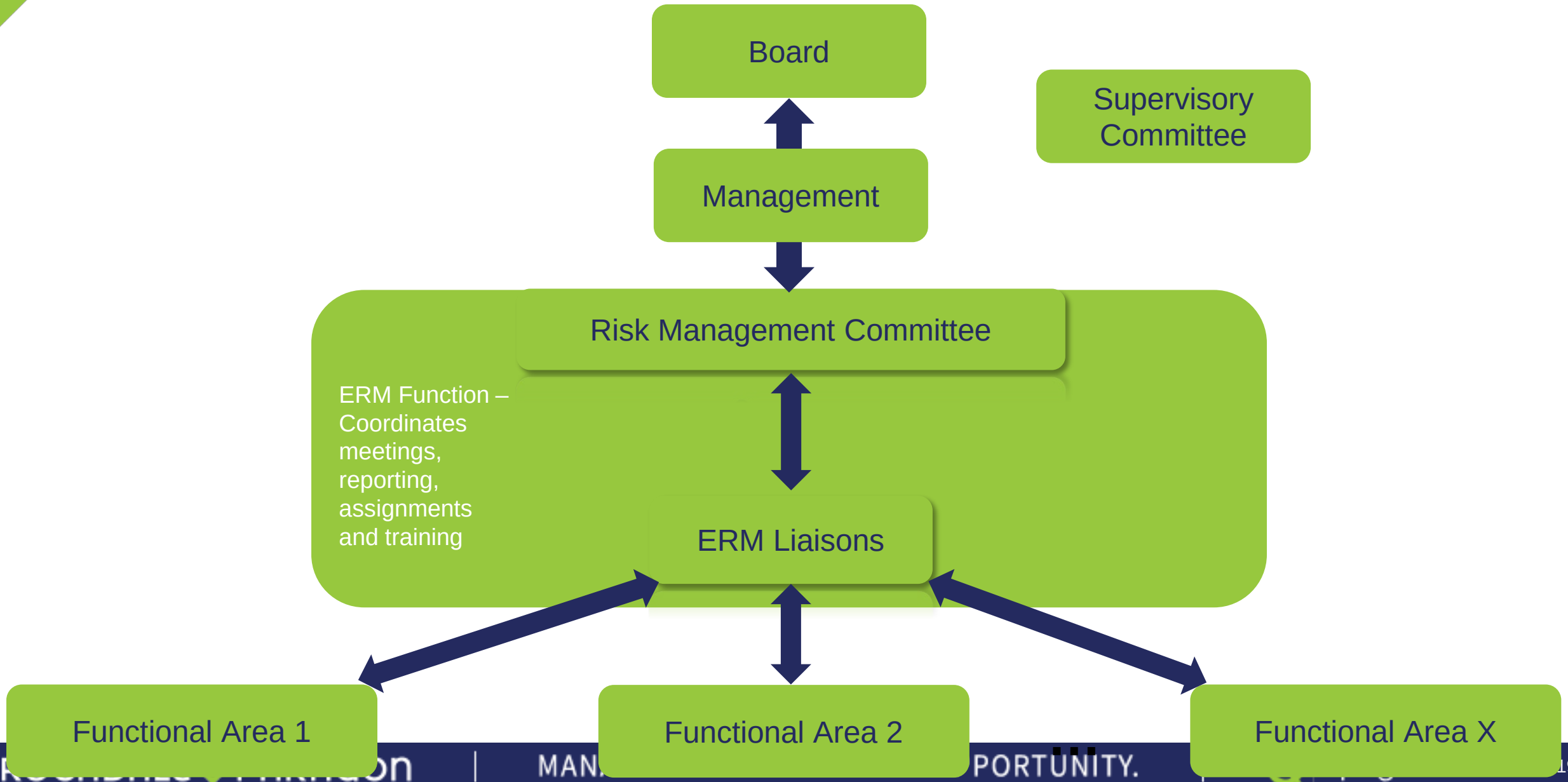
Risk Appetite Best Practices

- Include risk appetite material in board materials
- Tie to strategic planning efforts
- Monitor activities for consistency with appetite
- Track metrics related to appetite ranges
- Discuss in risk management committee meetings
- Ensure strategies in ALCO, investment committee, credit committee and other settings are consistent with appetite
- Review every year or two and adjust accordingly

Best Practices in Risk Identification

- Identify the key risks in functional areas, projects, processes and products:
  - Exposures, uncertainties and missed opportunities
- Consider internal and external factors
- Develop scenarios to demonstrate the risks
- Assess risks using consistent quantitative scales for impact, likelihood, and completeness of mitigation
- Strive to have risk profiles that represent managers' views of the key risks

ERM Information Flow



Risk Management Committee

- Demonstrate appropriate risk culture and tone
- Provide cross-functional input on risk identification and assessment
- Identify, discuss and act on risk issues
- Evaluate risk levels in the context of risk appetite
- Provide input for board and other reporting
- Improve the ERM process at the credit union over time:
  - Think about the RMCO meetings as time dedicated to discussing risk issues and opportunities that might have a significant impact on the credit union

The Board's Role

- Support risk culture and tone
- Discuss, understand and affirm risk appetite
- Review strategy against portfolio view of risk
- Understand how management identifies, communicates and mitigates key risks
- Question and challenge the ERM process

Lines of Defense

1 Line of Business

- Owns and manages risks
- Establishes appropriate risk processes and programs
- Identifies and escalates risk issues
- Identifies new opportunities

2 Risk Management

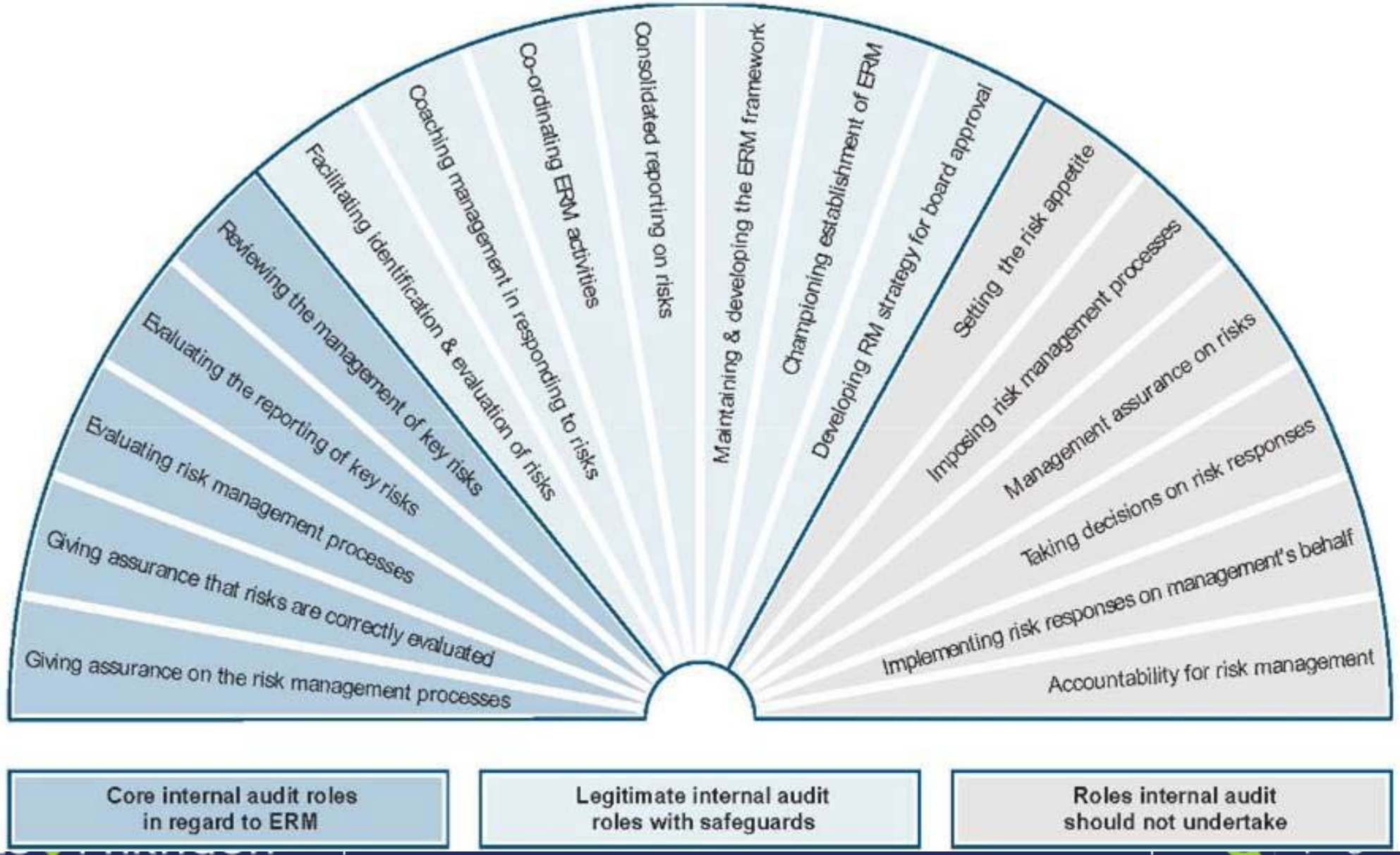
- Sets risk limits
- Quantifies and monitors risks
- Challenges risks and mitigating actions
- Aggregates risks across organizational boundaries

3 Internal Audit

- Validates risk programs
- Reports on risk management effectiveness

Role of Internal Audit

Source: https://na.theiia.org – "The Role of Internal Auditing in Enterprise-wide Risk Management"



Value = Meeting more of your objectives more of the time!

- Enhance strategy by considering risk and appetite
- Improve strategy execution
- Improve risk / return relationships
- Minimize negative surprises
- Improve organizational alignment
- Identify more opportunities

ERM Process Summary

- ERM is a process not a project
- Make it a small part of everyone's day-to-day duties and thought process:
  - "Culture eats strategy for lunch"
- Involves a variety of key periodic steps
- Use ERM to enable rather than impede actions

ERM Program Review

Purpose of ERM Program Review

- Measure the credit union's ERM program against best practices
- Identify opportunities for enhancements
- Ensure risk identification and assessment processes are reasonable

Approach of Review

- Conduct interviews with key participants in the ERM process:
  - CRO/Risk Manager
  - CFO
  - CEO
  - Other member of RMCO
  - Board member
- Organize and analyze interviews by the five COSO components and 20 underlying principles:
  - Consider using a questionnaire and consistent rating scale
  - Document the comments from the interviews

Approach of Review

- Review a variety of ERM program materials:
  - ERM Policy
  - Board and senior management reports
  - ERM committee materials
  - Risk appetite materials
  - Other documents
- Try to identify opportunities to enhance the materials to more completely meet the needs of key users, as identified earlier in the interviews:
  - Highlight areas where the materials may not be “best practice”
  - However, there is no one ideal ERM program

ERM Program Review Output

- Summarize your findings:
  - Ratings of COSO interview topics
  - Key strengths and weaknesses, including interview comments
  - Opportunities to enhance the ERM process
  - Opportunities to improve ERM reporting
- Discuss the results with ERM personnel
- Identify the key takeaways and timeline for actions
- Follow up to ensure improvements are implemented

Common ERM Opportunities

- Unclear objectives:
  - Confusion on roles and benefits
- Infrequent or sporadic risk updates/reporting – Inability to use timely information and deterioration of ERM culture
- Use of only qualitative ERM assessment scales:
  - Does not force quantitative risk decisions
- Lack of risk appetite development and monitoring:
  - How can we make good decisions if we've never thought about appetite?
- Failure to consider risk in strategy setting:
  - Let's use our risk information to minimize uncertainty in decisions

ROCHDALE PARAGON | apogee iQ

MANAGING RISK. SPOTTING OPPORTUNITY.

Questions?

Thank you!

Scott Hood

913-890-8014

shood@rochdaleparagon.com