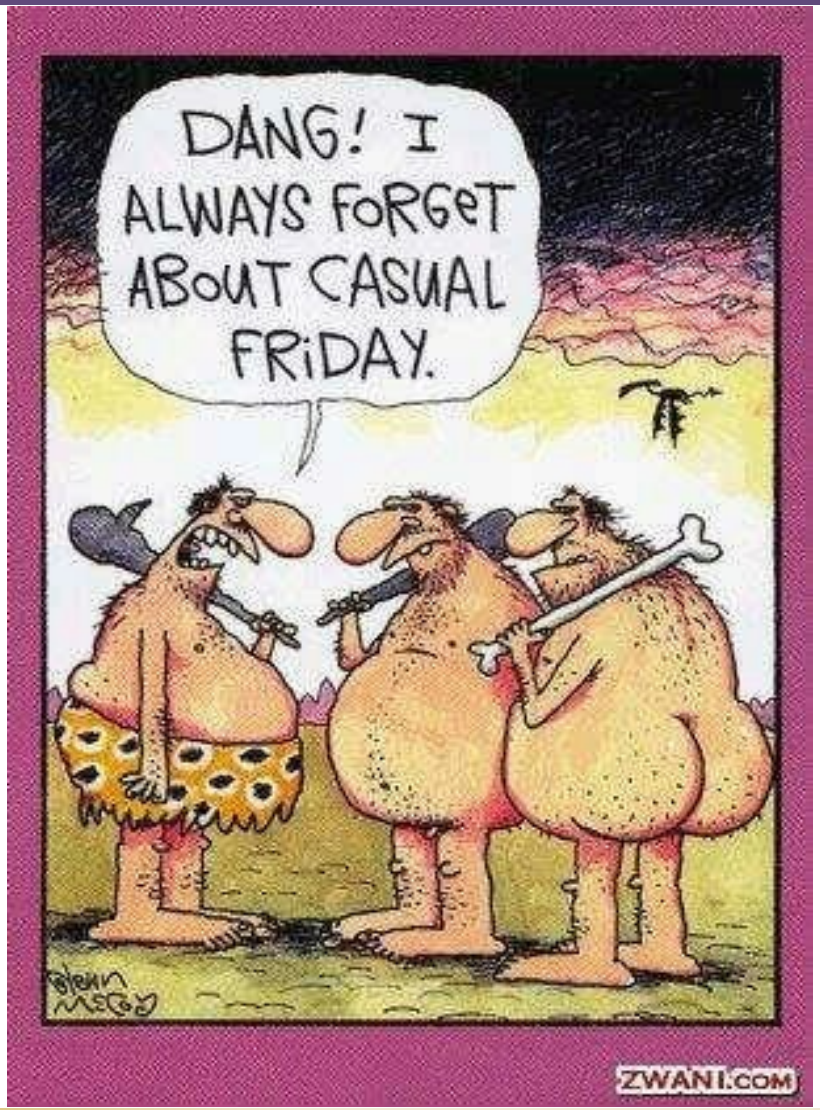
Enterprise Risk Management Integrating with Strategy and Performance: The Auditor's Role

Joe Maleszewski, Vice President for Audit
Florida Agricultural and Mechanical University
August 25, 2021

Presentation Outline

- Risk
- Risk Management
- Enterprise Risk Management
- Risk Management Frameworks
- COSO ERM Framework
- Role of Audit
- Q&A

RISK: AS OLD AS TIME



Risk Defined

Risk is the probability that an event will occur and adversely affect the achievement of objectives.

Risk Assessment Defined

Risk Assessment is the identification and analysis of risks to the achievement of an organization's objectives for the purpose of determining how those risks should be managed.

TRADITIONAL RISK MANAGEMENT V. ERM

Traditional Risk Management	Enterprise Risk Management
Past-focused	Future-focused
Segmented/Siloed	Enterprise-wide
Little or no knowledge of overall organizational risks	Broad perspective on overall organizational risk
Focused on preventing loss within business unit (tactical)	Focused on enhancing value, capitalizing on opportunities, and managing all risks across entire organization (strategic)
Scope: physical and financial assets	Scope: entire asset portfolio
Siloed risk mitigation	Enterprise-wide risk mitigation

ERM Milestones

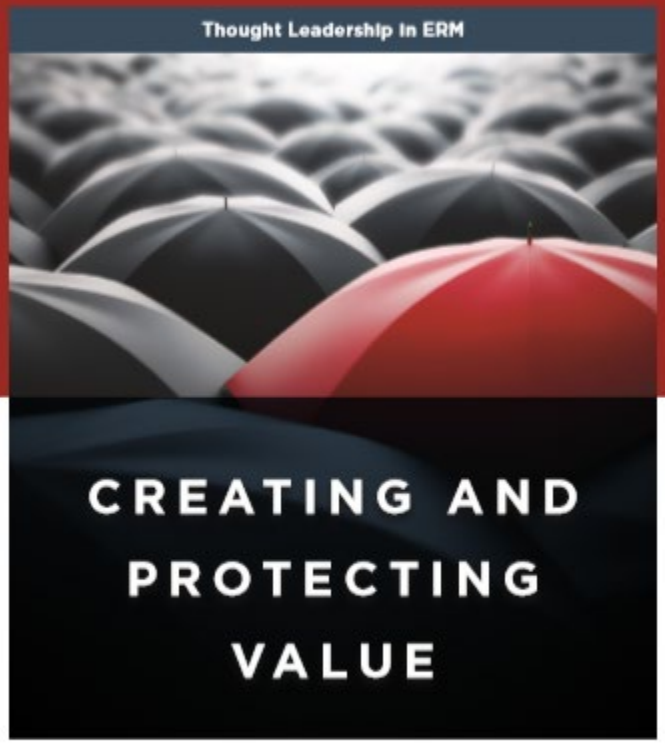
YEAR	MILESTONE
1900s	Risk Management: Logical, disciplined approach to future uncertainties
1974	Gustave Hamilton Risk Management Circle
1987	COSO: Report on Fraudulent Financial Reporting
1992	COSO: Internal Controls: Integrated Framework Cadbury Report: Financial Aspect of Corporate Governance CoCo: Canadian Institute of Chartered Accountant's Criteria for Control Framework
1993	Chief Risk Officer
1995	First Risk Management Standard: AS/NZS 4360
1996	COBIT: IT Governance
1999	GAO: Standards for Internal Control in Federal Government
2004	COSO: ERM – Integrated Framework
2009	ISO 31000: Suite of Risk Management Standards
2016	OMB: Circular A-123 requires Federal Agencies to implement ERM and Internal Controls
2017	COSO: ERM – Integrating with Strategy and Performance

About COSO . . .

- Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM), internal control, and fraud deterrence.

COSO

Committee of Sponsoring Organizations of the Treadway Commission

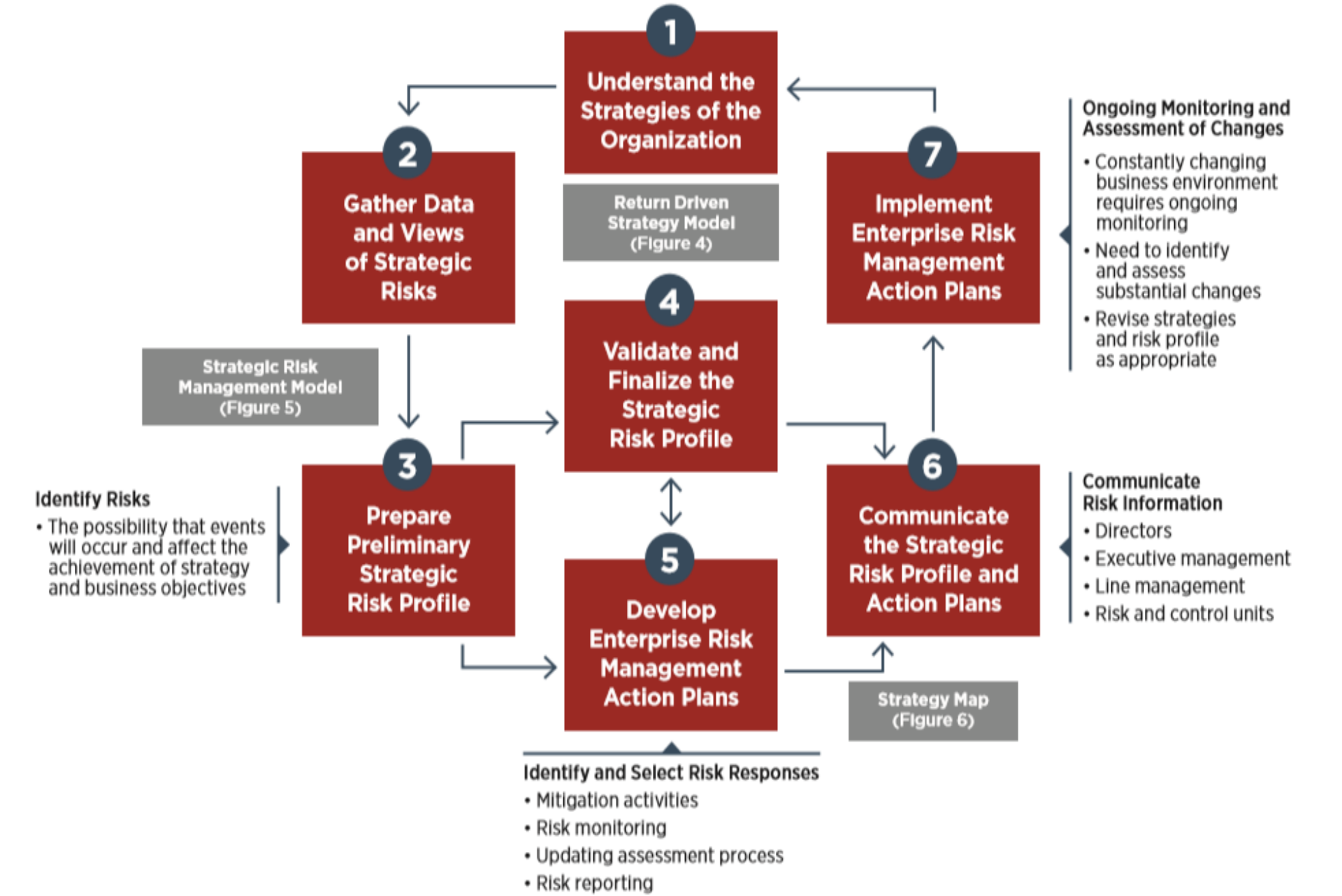


UNDERSTANDING AND IMPLEMENTING ENTERPRISE RISK MANAGEMENT

By

Richard J. Anderson | Mark L. Frigo

Figure 3. Strategic Risk Assessment Process



Source: Adapted from Frigo, Mark L., and Richard J. Anderson. "Strategic Risk Assessment: A First Step for Risk Management and Governance." Strategic Finance (December 2009) and Frigo, Mark L. and Richard J. Anderson, *Strategic Risk Management for Directors and Management Teams* (2011). Used with permission.

Renewed Focus on ERM

- Economic Recessions and Corporate Scandals
- Constant Change in Operational Environment – New Threats and Vulnerabilities
- Increasing Public Scrutiny
- Increasing Expectations from Government (Do More with Less)
- Increasing Compliance Requirements

What is ERM?

- Enterprise Risk Management (ERM) is defined by the Committee of Sponsoring Organizations (COSO) 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 entity objectives."

ERM…

- Provides a comprehensive and systematic approach to more proactive and holistic risk management
- Provides a common lexicon of risk terminology, and provides direction and guidance for implementing ERM
- Requires that organizations examine their complete portfolio of risks, consider how those risks interrelate, and that management develop an appropriate risk mitigation approach to address these risks in a manner consistent with the organization's strategy and risk appetite

ERM PROGRAM CHARACTERISTICS

- Enterprise-wide approach
- Executive-level sponsorship
- Defined accountability
- Intentional
- Systematic and structured
- Defined risk appetite
- Establishment and communication of risk management process goals and activities
- Monitored treatment plans

ERM is not…

- A silver bullet to prevent risks from occurring
- A methodology or a checklist of items that need to be completed that guarantee results
- The only way organizations can take a more proactive approach to managing risk

ERM Challenges

- ERM is too costly to implement!
- Current staff already have a huge workload!
- We don’t have resources for ERM!
- How do staff know what risks ***they*** “own?”
- We already do risk assessments!

Key Reminders

- Each organization is unique.
- Each organization needs a tailored approach.
- ERM is not a compliance exercise.
- ERM is a mindset.
- ERM facilitates information-sharing.
- ERM facilitates decision-making.

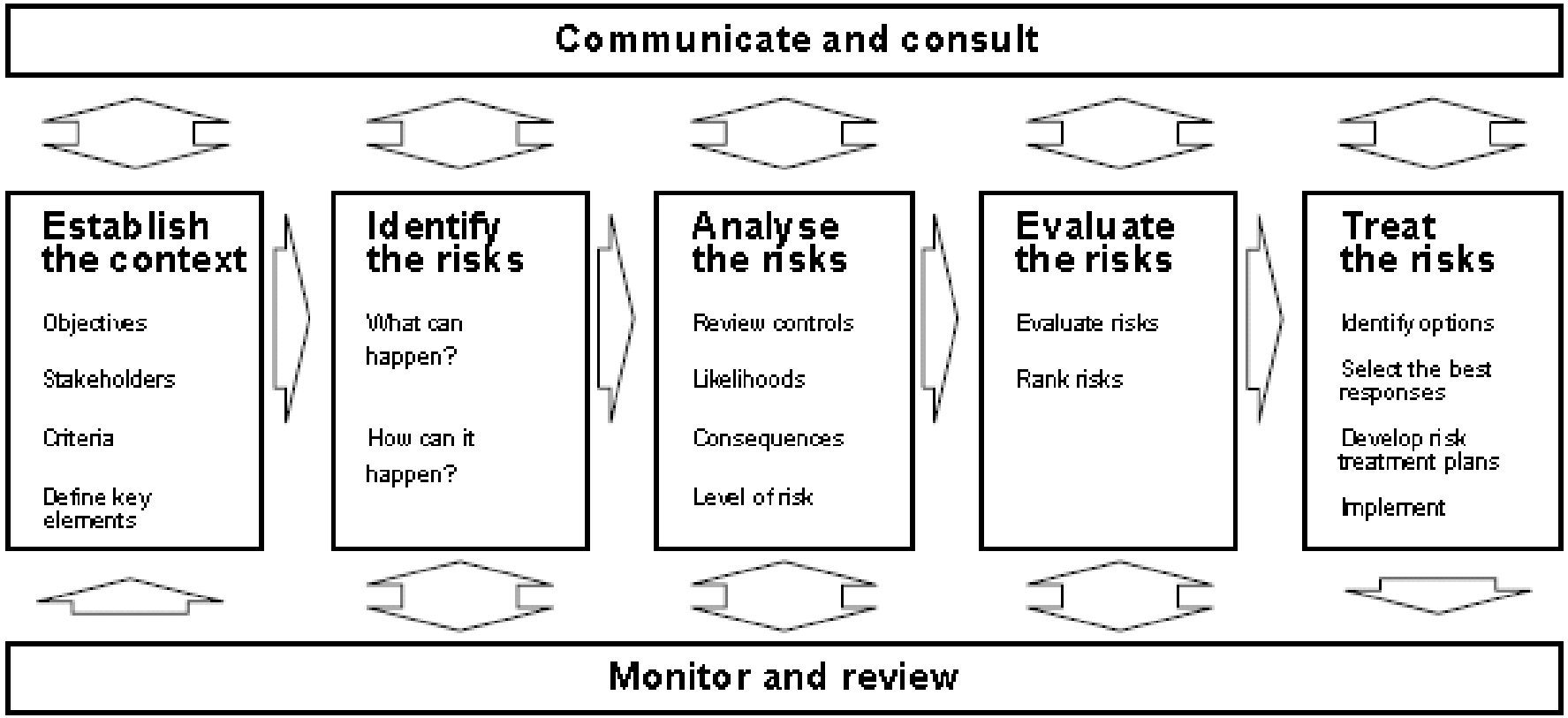
Where's the Value???

- The biggest value in ERM frameworks lies in their promotion of continuous improvement, diligent management practices, and ongoing monitoring.

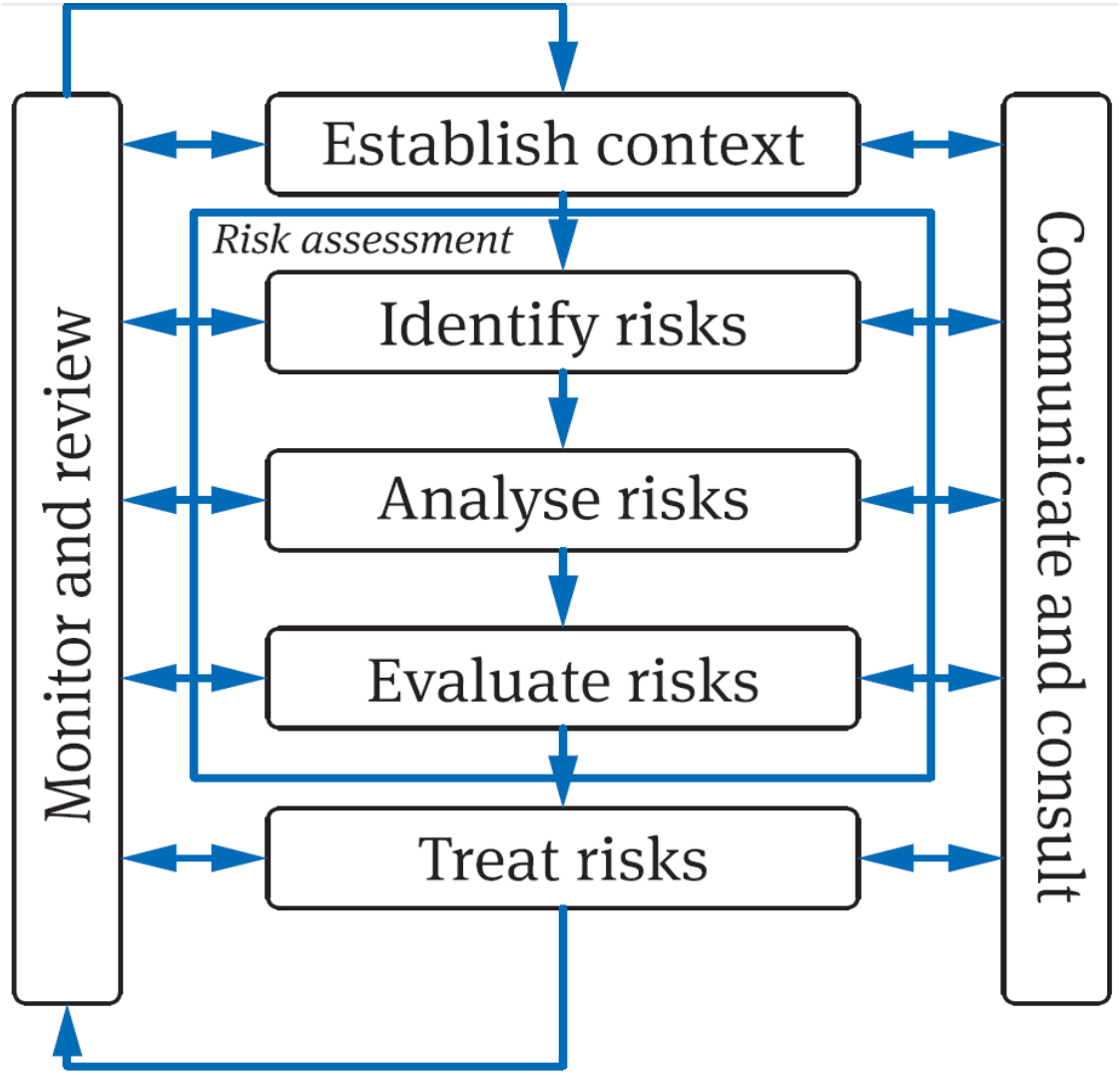
RISK MANAGEMENT FRAMEWORKS

FRAMEWORK	DESCRIPTION
AS/NZS 4360	Australian and New Zealand Standard on Risk Management (1995)
ISO 31000	International Organization for Standardization (ISO) based on AS/NZS 4360
COSO	Enterprise Risk Management Framework: Integrating with Strategy and Performance (2004 ⇨2017)

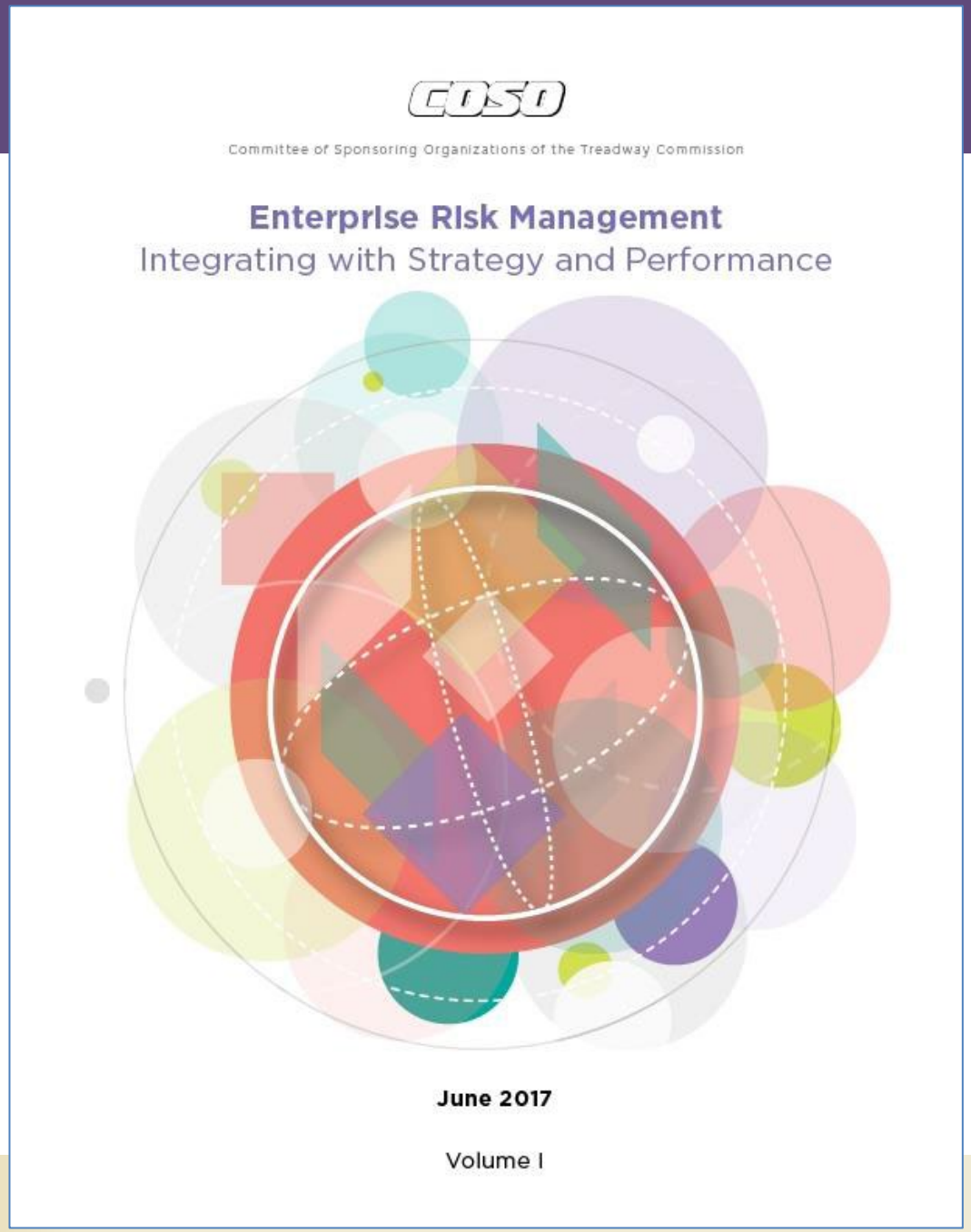
AS/NZS Framework



ISO 31000 – Framework



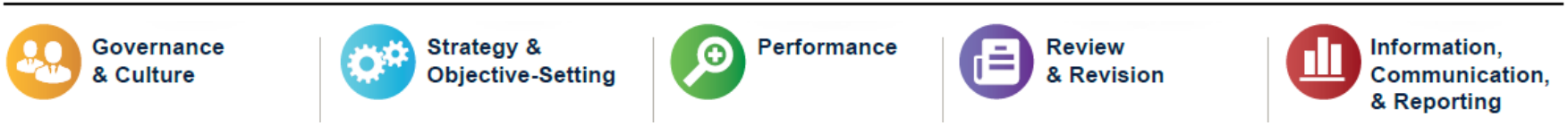
Enterprise Risk Management Framework: Integrating with Strategy and Performance (June 2017)



- 10 Key Things to Know about the Framework

1) Provides a New Document Structure

- Framework focused on fewer components (five)



- Uses focused call-out examples to emphasize key points
- Follows the business model versus isolated risk management process

2) Introduces Principles

- 20 key principles within
- each of the five components

Governance & Culture

1. **Exercises Board Risk Oversight** - Board of directors provides oversight of strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.

2. **Establishes Operating Structures** - Organization establishes operating structures in the pursuit of strategy and business objectives.

3. **Defines Desired Culture** - Organization defines desired behaviors that characterize entity's desired culture.

4. **Demonstrates Commitment to Core Values** - Organization demonstrates commitment to entity's core values.

5. **Attracts, Develops, and Retains Capable Individuals** - Organization committed to building human capital in alignment with strategy and business objectives.

Strategy & Objective-Setting

6. **Analyzes Business Context** - Organization considers potential effects of business context on risk profile.

7. **Defines Risk Appetite** - Organization defines risk appetite in context of creating, preserving, and realizing value.

8. **Evaluates Alternative Strategies** - Organization evaluates alternative strategies and potential impact on risk profile.

9. **Formulates Business Objectives** - Organization considers risk while establishing business objectives at various levels that align and support strategy.

Performance

10. **Identifies Risk** - Organization identifies risk that impacts performance of strategy and business objectives.
11. **Assesses Severity of Risk** - Organization assesses risk severity.
12. **Prioritizes Risks** - organization prioritizes risks as basis for selecting risk responses.
13. **Implements Risk Responses** - Organization identifies and selects risk responses.
14. **Develops Portfolio View** - Organization develops and evaluates portfolio view of risk.

Review & Revision

15. **Assesses Substantial Change** - Organization identifies and assesses changes that may substantially affect strategy and business objectives.

16. **Reviews Risk and Performance** - Organization reviews entity performance and considers risk.

17. **Pursues Improvement in Enterprise Risk Management** - Organization pursues improvement of enterprise risk management.

Information, Communication, & Reporting

18. **Leverages Information Systems** - Organization leverages entity's information and technology systems to support enterprise risk management.

19. **Communicates Risk Information** - Organization uses communication channels to support enterprise risk management.

20. **Reports on Risk, Culture, and Performance** - Organization reports on risk, culture, and performance at multiple levels and across entity.

3) Incorporates New Graphics

- Graphic has stronger ties to the business model

4) 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

5) Emphasizes Value

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

6) Links to Strategy

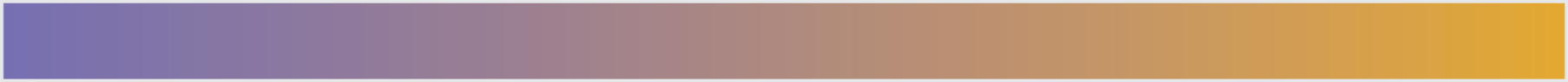
- Explores strategy from three perspectives:
  - Possibility of strategy and business objectives not aligning with mission, vision and values
  - Implications from the strategy chosen

7) Links to Performance

- Enables 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 risk identification and assessment that impact performance
  - Discussing tolerance for variations in performance
- Manages risk in the context of achieving strategy and business objectives – not as individual risks

8) 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 broader context of overall core
- Depicts culture behavior within a risk spectrum



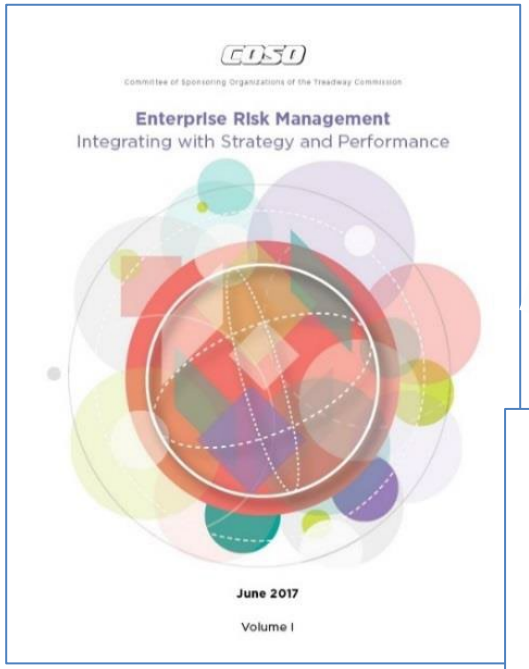
- Explores possible effects of culture on decision-making
- Explores alignment of culture between individual and entity behavior

9) 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 risk profile

10) Builds links to internal control

- Document does not replace the *Internal Control –Integrated Framework*
- The frameworks are distinct and complementary
- Both use a components-and-principles structure
- Aspects of internal control common to enterprise risk management are not repeated
- Some aspects of internal control are developed further in this framework



Role of Audit

- Renewed Focus on ERM
  - More diverse, complex risks
  - More opportunities for IA to lead
- The Evolving Role of Internal Audit
  - Educator
  - Consultant
  - Independent assurance provider
- Drawing the Boundaries
  - Distinguish decision-making from consulting/advisory Role
  - Communicate to all involved

Definition of Internal Auditing

- "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes."

Governance, Control, and Risk Management

Governance	• Strategic and operational decision-making • Overseeing and communicating risk management and control information • Promoting organizational ethics and values • Ensuring effective organizational performance management and accountability • Coordinating with the board, external and internal auditors, other assurance providers, and management
Control	Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
Risk Management	A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

Risk Management and Standards

- **IIA Standard 2120 – Risk Management**
- The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.

- 2120.C3 – When assisting management in establishing or improving risk management processes, internal auditors must refrain from assuming any management responsibility by actually managing risks.

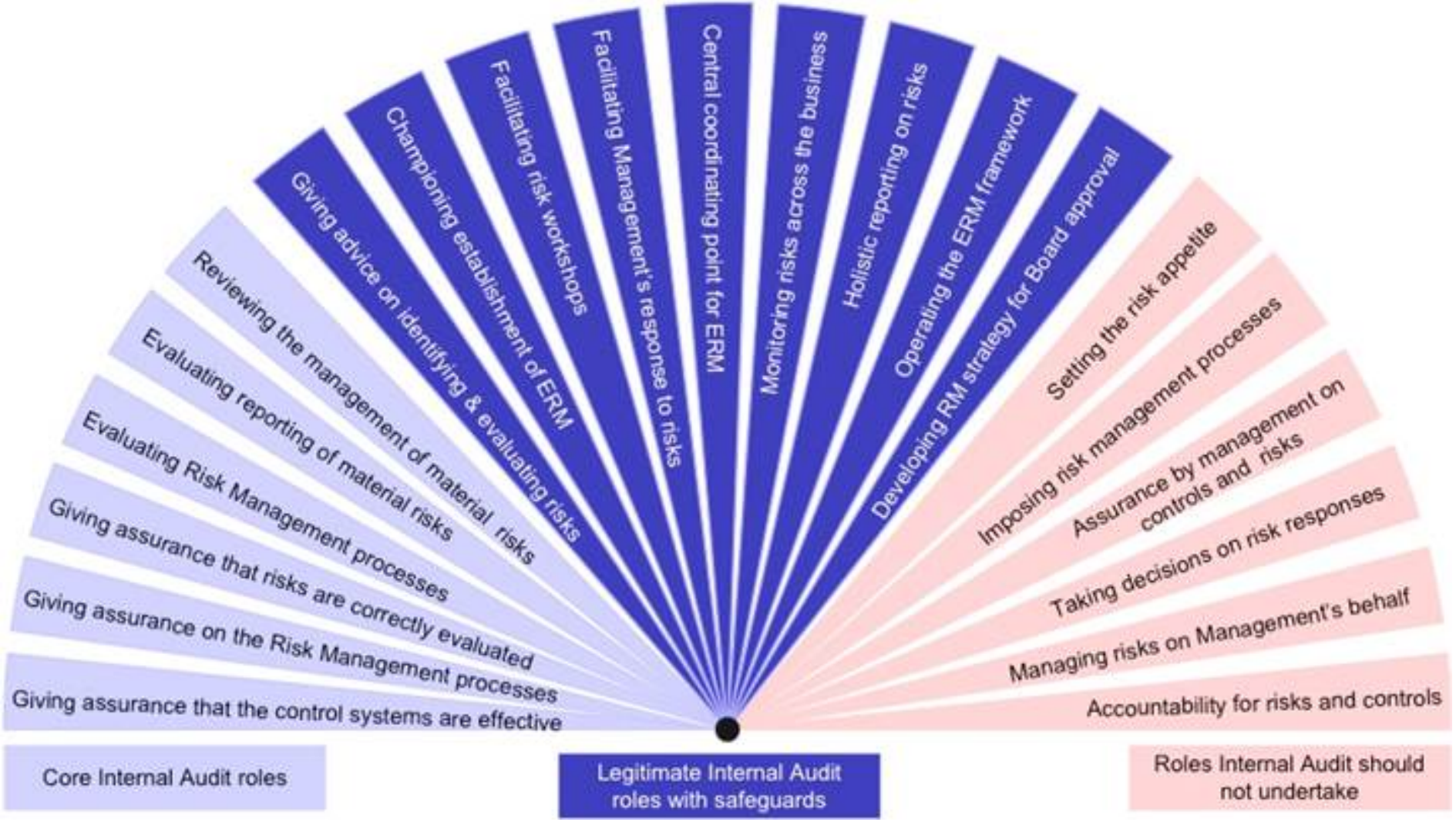
When Lines May be Blurred

- Facilitating risk assessments/workshops
- Coaching/educating management
- Coordinating ERM activities
- Maintaining the ERM framework
- ERM Champion
- Developing ERM strategy for leadership

What to Avoid

- Helps the organization set the risk appetite.
- Develops policies or risk management processes.
- Determines the appropriate risk response.
- Implements risk responses.
- Ownership/accountability for risk management functions.

Internal Audit – Role in ERM



Summary

- Risk
- Risk Management
- Enterprise Risk Management
- Risk Management Frameworks
- COSO ERM Framework
- Role of Audit
- Q&A

Questions/ Comments