Are you prepared for this Challenge? The new COSO Enterprise Risk Management Framework

CAGFO 2018 Conference Winnipeg, MB

September 13, 2018; 10:30am

pwc

Agenda

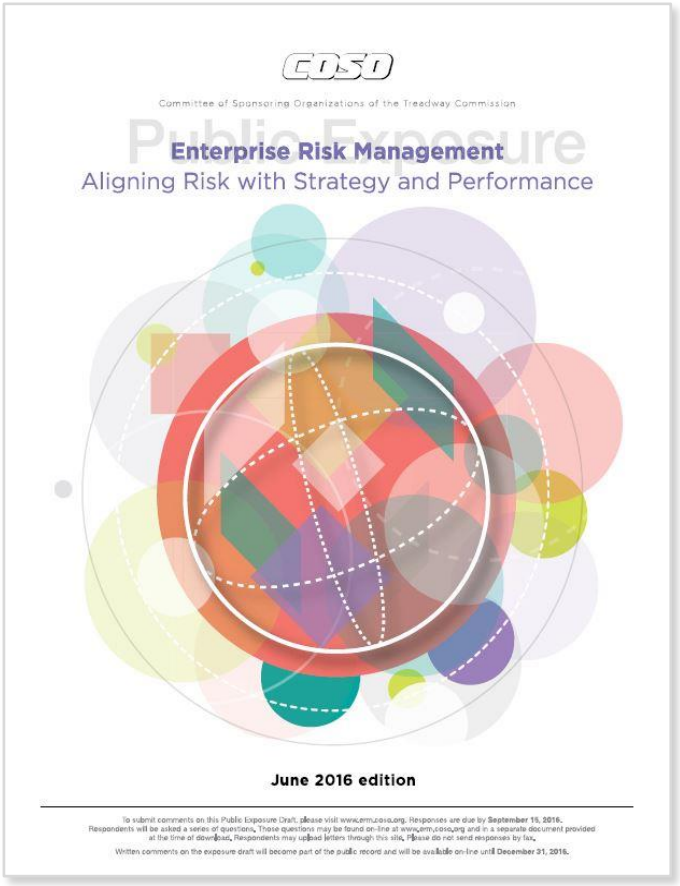
01	*What is being said of ERM today?*
02	*What has changed in the new COSO ERM framework?*
03	*How can you enhance ERM in your organization?*
04	*Where should you start? Where can you find more information?*

01 What is being said of ERM?

So what are we hearing?

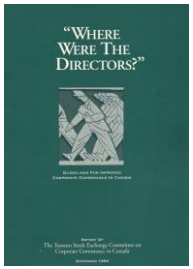
Leadership Recognizes - There are Opportunities for ERM to add Greater Value

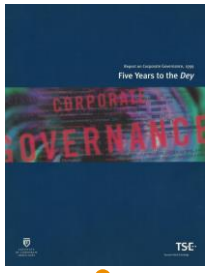
What is COSO ERM 2017?



- **Leadership is expecting more** from their organisation's ERM practices and capabilities
- Stakeholders are seeking **greater transparency** and accountability
- Political and business **environments are increasingly complex,** technologically driven, and global
- There is a need to **incorporate lessons learned** from recent events and the bar is rising
- Risk professionals are looking for a **more up to date resource** describing ERM concepts
- The range of ERM **practices continues to evolve**

Evolution of Risk Management & Other Models



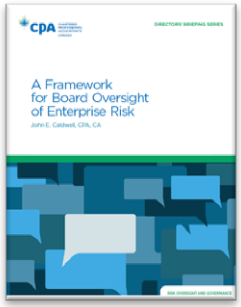


Dey Report 1994
Dey report sets out expectations of directors following several high profile company failures

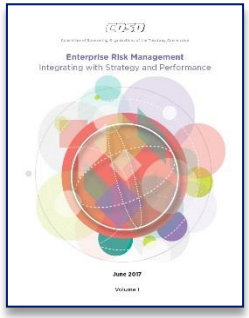
Five years to the Dey (1999)
Follow up on progress made following Dey report recommendations

ERM/RM Frameworks (2004 – 2008)
enter market:
- COSO
- ISO
- Treasury Board

SOX/ 52-109 (2005/2008)
Internal control certification requirements set



CPA Canada (2012)
CPA Canada issues its guidance on the role of the board in overseeing risk



COSO ERM (2017) and ISO (expected early 2018) updated

Handbook on Board Governance released (2016)
This 800 page volume on governance includes 50 pages on risk management oversight

02 What has changed in the new COSO ERM framework?

A new definition

Enterprise risk management is defined as:

The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value.

Source: COSO Enterprise Risk Management-Integrating with Strategy and Performance

A new framework structure

The graphic symbolizes the dynamic, integrated nature of ERM that begins with the mission, vision and core values of the organization through to the creation of enhanced value.

5

Components that align to the business life cycle

20

Supporting principles that collectively describe the ERM Framework

What changed?

03 How can you enhance ERM in your organization?

10 considerations in getting started

Adopt a principles-driven view of ERM –applying principles that align to the business lifecycle, making risk conversations more intuitive for your organization

Explore the different benefits of ERM–consider the spectrum from loss mitigation through to strategic advisor and how they inform the practices within the organization

Link risk management into strategy– link risk with strategy setting, using ERM principles to support the creation, realization, and preservation of value

Explores managing risk at all altitudes of the organization–from entity level through to procedural level risks, make ERM more than just an isolated view of risk in the business and something that resonates with the board

Communicate from the perspective of the business–discuss risk management concepts in terms of helping your organization create value, enabling you to realize true benefits from ERM

Emphasize on culture– reflect on the changing demands and expectations of today's markets, helping your organization make responsible risk decisions

Have deeper discussions on risk appetite–have meaningful conversations on risk appetite and how

Address the evolving role of technology in managing risk– explore the evolving role of technology's influence on managing risk

Shift assessments from risk centric to performance oriented–explore ways to evolve beyond lists and heat maps to provide true insights into risk's impact on performance

Consider your reporting–explore how current risk reporting is providing insight to the users

Adopt a principles driven approach

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

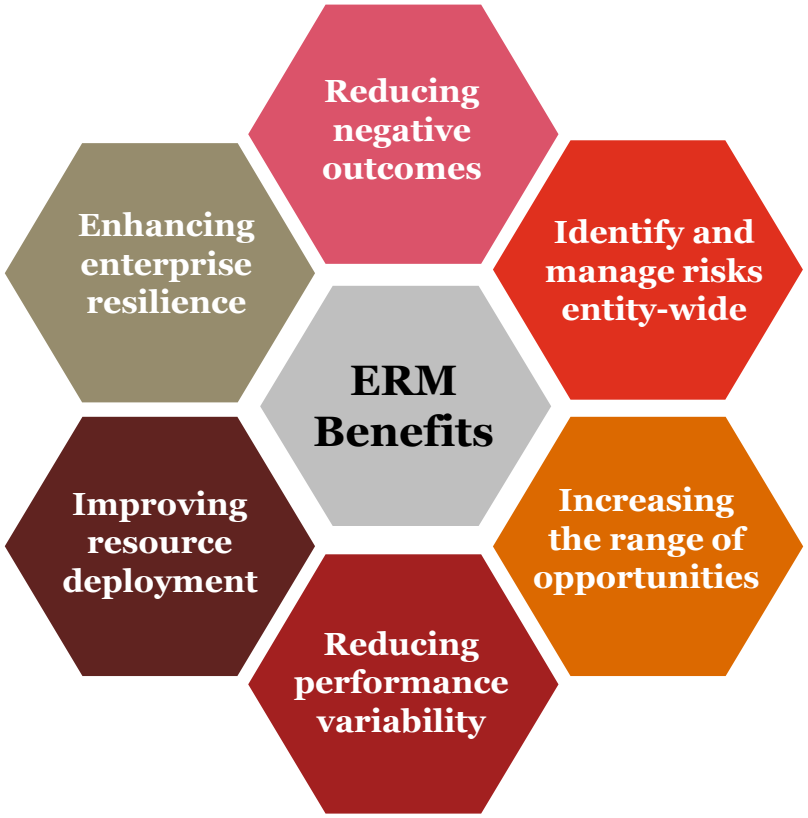
Considerations in getting started

- Delve into the 20 COSO principles and what they say – not what you think they might say
- Consider how these principles are applied today, and how they might shape the future evolution of your practices and capabilities
- Assess the maturity of your current practices and the value that these practices provide across the organization (principles based assessment vs maturity assessment)

Considerations in getting started

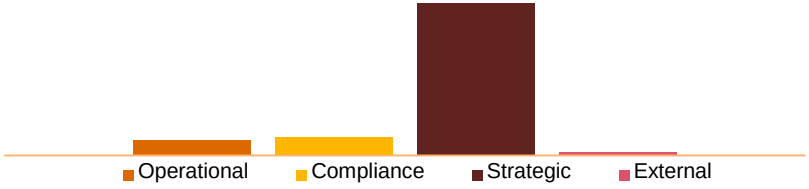
- Explore with Council and administrative leadership which of these benefits should have higher focus
- Evaluate current practices in place to determine the actual benefits you should expect of your ERM efforts

Explore the different benefits of ERM



ERM is not a "one-size-fits-all" program – activities must be tailored to align with the benefits

Link risk management into strategy



Studies have revealed that the strategy setting process is a critical area of integration for ERM

- Strategic blunders account for a majority of the losses in shareholder value compared to operational events, incidents or compliance failures
- Research suggests that organizations are looking to strengthen the integration between strategy and enterprise risk management

81% of the greatest losses in stakeholder value since 2002 were attributable to 'strategic blunders'

Considerations in getting started

- Consider how ERM fits into the overall strategy setting process (as a capability, not a function) – are you focused on the 80% or the 20%?
- Review your own strategic blunders/near misses to reduce such reoccurrences in the future
- Summarize the most significant assumptions underpinning your strategy and the possible effect on performance should these assumptions change
- Identify what triggers exist today that alert you when its time to revisit strategy

Link risk management with strategy

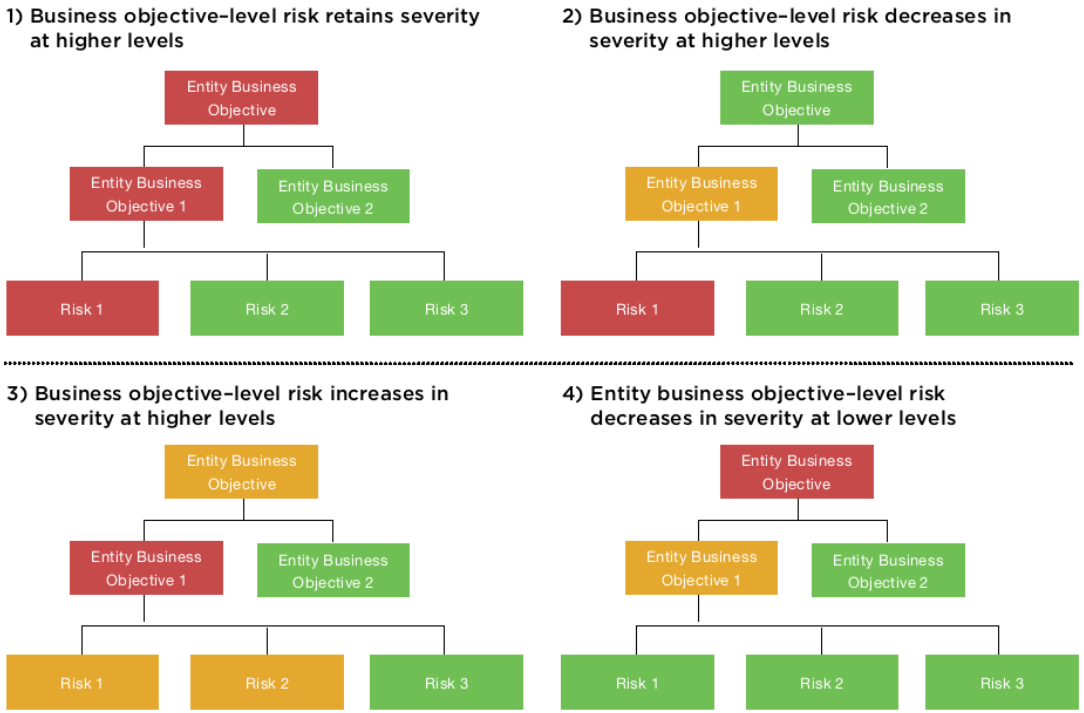
Integrating strategy and risk through three different dimensions

1. The possibility of strategy not aligning with mission, vision and core values
2. The implications from the strategy chosen
3. Risk to strategy and performance

Considerations in getting started

- Review the governance model in place and the ability to interpret risks at all levels
- Review reporting at each level – from day to operations up to Council– and the clarity in communicating risk in relation to performance at each level
- Evaluate capabilities for identifying risks at all levels and the rigor in assessing those risks as they move through various levels

Explore managing risk at all altitudes of the organization



Risks emanate and must be managed at all levels of the organization. ERM needs to explores how risks can manifest at multiple levels within an organization with some risks directly impacting the entity strategy while others impacting business objectives.

Risks can change in severity and prioritization at different levels of the organization and how the impacts of correlation and diversification are considered when analyzing the risk profile of portfolio view of risk.

Communicate from the perspective of the "business"

ERM needs to resonate from the perspective of key stakeholders to gain acceptance and adoption throughout the organization

- Research has confirmed that there is often a **'siloed' approach** to risk that is separate from the day to day management of an organization
- Risk management is perceived as an **incremental activity** performed by those independent or outside of the "business"
- The lack of integration can contribute to **difficulties engaging with the service delivery lines**, the ability to gain and offer insight and ultimately curbs the value that ERM can offer
- Consider ways to better link risks with performance
    - How is risk and performance inter-related?
    - How does risk relate to over and/or under performance?

Considerations in getting started

- Look at your risk management reporting, policies, standards – are they written from a risk management perspective or a "business" perspective?
- Try this exercise: Write your reports without using the words "risk" or "risk management"

Emphasize culture

Culture forms an integral part of ERM and is instrumental in influencing how people make decisions on managing risk

Culture is becoming **more focused on decision-making** and the alignment to expected behaviors in line with the core values of the organization

The importance of **aligning the core values and risk appetite** of the organization to promote consistent and risk-based decision making

Considerations in getting started

- Articulate both the desired and actual risk culture – Are you where you want to be?
- Consider where you have a healthy, natural tension that balances out the culture and where there may be an unhealthy, dominant culture in place
- Incorporate information and reporting of orgnizatioal culture in your ERM reporting

Have deeper discussions on appetite

- Risk appetite for many organizations is a challenge, and for some is simply "shunned" as part of ERM
- In practice, and when done well, it provides significant advantage in harmonizing decisions across the entity
- The relationship between appetite, tolerance, indicators and triggers

Appetite
- Applies through development of strategy and setting of objectives
- Focuses on overall goals of the business (objective-centric)
- Aids in decision-making and evaluation at the portfolio
- Ties strategy to measures

Tolerance
- Applies in the implementation of strategy
- Focuses on objectives and variation from plan (objective-centric)
- Aids in decision-making and in evaluation
- Ties strategy to measures

Indicators and triggers
- Applies at any level of the business
- Considers specific risks, usually in isolation (risk-centric)
- Ties risks to measures (e.g., key indicators)

Considerations in getting started

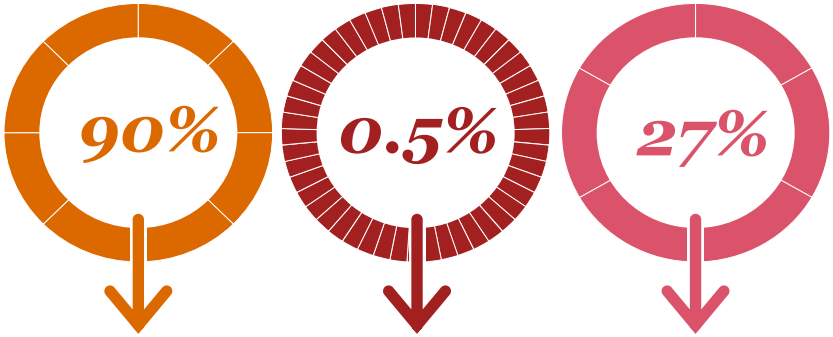
- Discuss whether an evaluative or decision-making approach best fits your organization needs
- Communicate risk appetite using business language, not risk-centric language
- Consider risk appetite in the context of risk profiles and portfolio view

Considerations in getting started

- Consider how technology could be used to capture better information to aid in decision-making
- Avoid the tendency to viewing technology as the entire approach for implementing ERM

Address the evolving role of technology in manging risk

The Framework recognizes the importance of enterprise risk management keeping pace with technological developments



Data Generation

Proportion of data that exists today was created in the past two years

Data Analysis

Only a small fraction of available data is currently analyzed

Impact on Industry

Percentage of CEOs that believe technology will completely reshape their industry

Source: PwC Mega Trends – Technological Breakthroughs

- ERM practices and capabilities need **to align with the velocity** of changes to the business context, emerging and changing risks
- Information, Communication and Reporting principles now have a greater focus **on integrated risk and performance reporting**
- Developments in **data generation and analytics** including 'big data', artificial intelligence and social media have been acknowledged
- Needs to consider the **accuracy, completeness and timeliness** of data

Shift assessments from risk centric to performance oriented

ERM practices focus on the potential for risk to impact **strategy and objectives** and the relationship to overall **performance**

The Framework considers how risk relates to performance

For instance, it explores the questions:

Does you understand the risk when setting your performance targets?

Have you performed as expected and achieved desired outcomes?

What risks are occurring that may be affecting performance?

Did you take enough risk to attain your desired outcomes?

Consider your reporting

- While reporting using the “tried and true” red/yellow/green risk lists and heat maps work in formative years, many organizations soon outgrow these approaches and want something better
- Too many Boards/Councils have disconnected from the risk management conversation as the reporting is not connecting to perfromance
- Focusing on improving these reports is not always the most effective use of resources, and it may be time to find a new way to report

Considerations in getting started

While many want the example of “good risk reporting”, try focusing first on performance and what matters to your stakeholders when they look at your organization. Then find the story that provides insight into how risk is, or might some day, shape that level of performance.

04 Where should you start? Where can you find more information?



Where to start next?

Some final thoughts on getting started

- While the above slides set out over 25 thoughts for getting started, we would suggest you select a smaller number and initially focus there – maybe 3-5
- Regardless of which one you choose:
  - Sync with the language of business in your organization
  - Envision both value preservation and creation throughout your organization

And a final word of caution

- Avoid viewing ERM simply as a function, team or department – the evolution of ERM will see risk capabilities extend far beyond a group of function
- Evolve your approach and reporting – the message is clear that boards and senior management want much more than a stand alone, periodic risk assessments and heat maps

Staying involved

Access the Framework at www.coso.org (with links to order on-line through either the IIA or AICPA)

View PwC videos, blogs and articles at https://www.pwc.com/gx/en/services/advisory/consulting/risk/coso-erm-framework.html

December 08, 2017

Episode 4: Risk Appetite - Delving into the world of decision-making and measurement

Organisations need to look at risk through the lens of business and using risk appetite to consider and evaluate risk can help to focus that picture.

November 22, 2017

Episode 3: Integrating risk and performance

Given that risk cannot be managed in isolation of performance and performance cannot be managed without consideration of risk, how can organisations integrate risk and performance?

October 31, 2017

Episode 2: Understand how risk conversations are changing and why

What's causing a shift in risk conversations and how can that dialogue help an organisation derive more value from enterprise risk management?

September 25, 2017

Episode 1: What you need to know about the new COSO ERM Framework

Discover what's changed in the new COSO ERM Framework and how those changes will impact the culture, capabilities and practices relied upon by management to manage risks in achieving strategy, performance and the creation of value.

How to reach us…

Robert Reimer
PwC Partner, Risk Assurance Services
Tel: 1-204 926 2442
Robert.j.reimer@ca.pwc.com

Gerry Valois (Today's Presenter)
PwC Director, Risk Assurance Services
Tel: 1-204 926 2455
gerry.valois@ca.pwc.com

Erin Stephen
PwC Director, Risk Assurance Services
Tel: 1-780 441 6702
erin.stephen@ca.pwc.com

Thank you