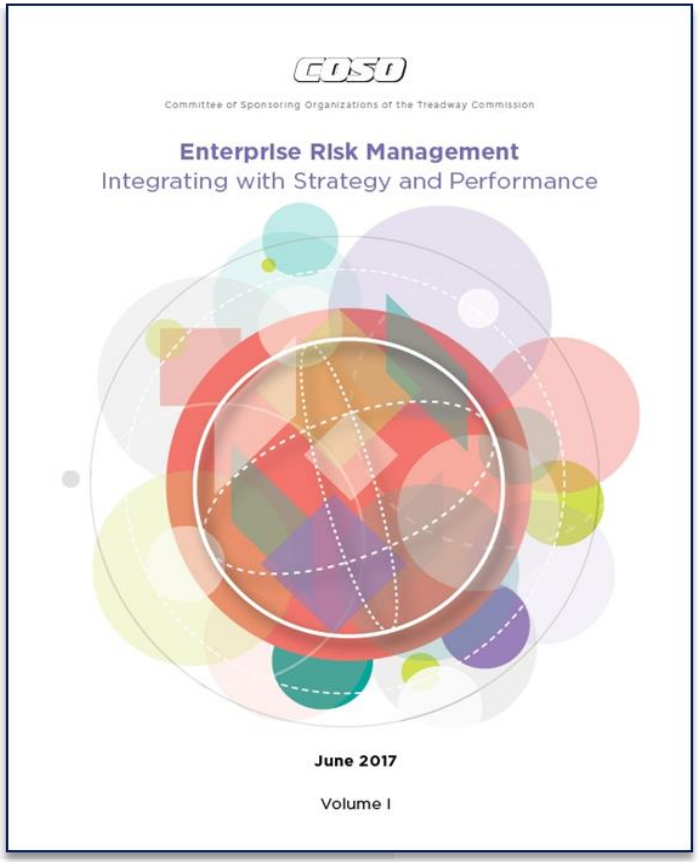
COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Enterprise Risk Management

Integrating with Strategy and Performance

Paul Sobel, Vice President / CAE
Georgia-Pacific, LLC
COSO Chairman

Jordan Reed, Managing Director, Protiviti



COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

ERM status quo: A focus on three questions

	Do we know what our key risks are?	Do we know how they're being managed?
	Key Objectives: • Delineate critical enterprise risks • Identify emerging risks in a timely manner • Provide sufficient visibility to ongoing business risks	Key Objectives: • Establish accountability for results in addressing: – Critical enterprise risks – Emerging risks • Establish and clearly communicate risk tolerances and limits • Provide transparency as to sources of assurance for ongoing business risks
	Expected Outcomes: • Focused board and executive management dialogue • Organization enabled to respond more in a timely manner to emerging issues	Expected Outcomes: • Clarity as to responsibility and accountability for managing risk • Escalation protocol to engender confidence in timely reporting of: – Breaches and near-breaches of risk tolerances and limits – Other significant issues warranting attention
How do we know?	• Effective criteria for assessing risk • Defined risk assessment process for identifying and prioritizing risks	• Transparency as to risk ownership • Effective risk reporting protocol
	• A repeatable process for identifying, prioritizing, mitigating and monitoring the most critical risks	

- The current state of ERM in most organizations is rooted in methods and processes from the 20th century
- ERM needs advancing to meet the challenges of a changing, uncertain and volatile world over the next five to 10 years
- The tools of the digital age are there but the state-of-the-art remains rooted in analog thinking

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Is the status quo enough?

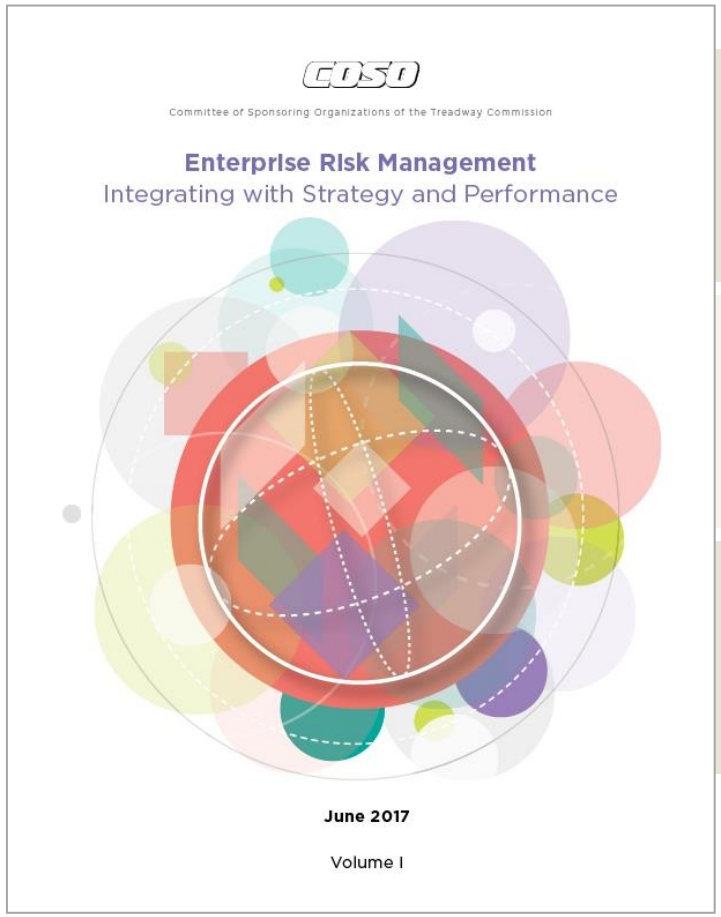
Questions management should ask:

- Is our ERM approach helping us identify flaws and weaknesses in our strategy on a timely basis?
- Is our organization able to recognize the signs of disruptive change, and is it agile and resilient enough to adapt?
- Do we truly consider risk and return in our decision-making processes or do we blindly follow the herd and remain emotionally invested in the comforts of our business model?
- Do we seek out what we don't know? Are we prepared for the unexpected?
- Is everyone competing for capital and funding with rose-colored glasses, making the resource and budget allocation process a grabfest?

Why was the Framework Updated?

- Concepts and practices have evolved
- Lessons learned
- Bar raised with respect to enterprise risk management
- Business and operating environments more complex, technologically driven, and global in scale
- Stakeholders more engaged, seeking greater transparency and accountability
- Risk discussions increasingly prominent at the board level

A New Title…



Retitled as *Enterprise Risk Management—**Integrating** with Strategy and Performance*

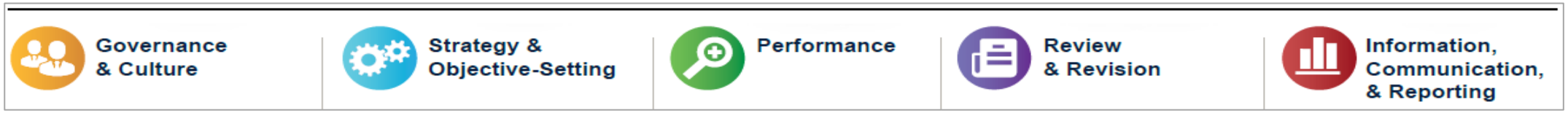
Recognizes the importance of strategy and entity performance

Further delineates enterprise risk management from internal control

10 Key Things to Know about the Framework

1) Provides a New Document Structure

Framework focused on fewer components (five)



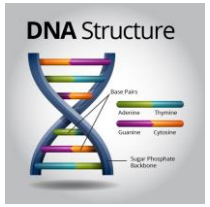
- Uses focused call-out examples to emphasize key points (> 30)
- Follows the business model versus an isolated risk management process

2) Introduces Principles

20 key principles within each of the five components

Governance & Culture	Strategy & Objective-Setting	Performance	Review & Revision	Information, Communication, & Reporting
1. Exercises Board Risk Oversight	6. Analyzes Business Context	10. Identifies Risk	15. Assesses Substantial Change	18. Leverages Information and Technology
2. Establishes Operating Structures	7. Defines Risk Appetite	11. Assesses Severity of Risk	16. Reviews Risk and Performance	19. Communicates Risk Information
3. Defines Desired Culture	8. Evaluates Alternative Strategies	12. Prioritizes Risks	17. Pursues improvement in Enterprise Risk Management	20. Reports on Risk, Culture, and Performance
4. Demonstrates Commitment to Core Values	9. Formulates Business Objectives	13. Implements Risk Responses		
5. Attracts, Develops, and Retains Capable Individuals		14. Develops Portfolio View		

3) Incorporates New Graphics/Concepts



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:
  - 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 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

6) Links to Strategy

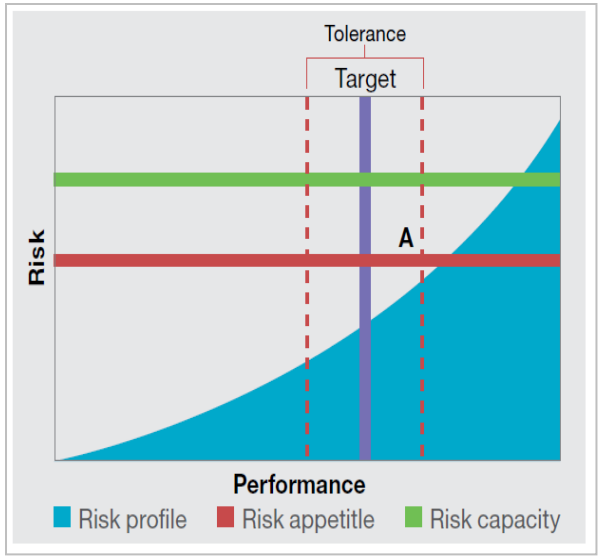
- Explores strategy from three different perspectives:
  - The possibility of strategy and business objectives not aligning with mission, vision and values
  - The implications from the strategy chosen
  - Risk to executing the strategy

7) 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

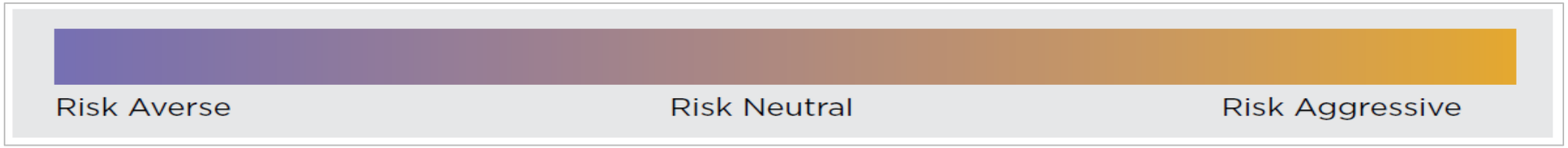
7) Links to Performance

- Introduces a new depiction referred to as a risk profile
- Incorporates:
  - Risk
  - Performance
  - Risk appetite
  - Risk capacity
- Offers a comprehensive view of risk and enables more risk-aware decision making
- The framework provides a complete depiction of how to build a risk profile in an appendix



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 the broader context of overall core values
- 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

Culture Eats Strategy for Breakfast

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 the risk profile

10) Builds Links to Internal Control

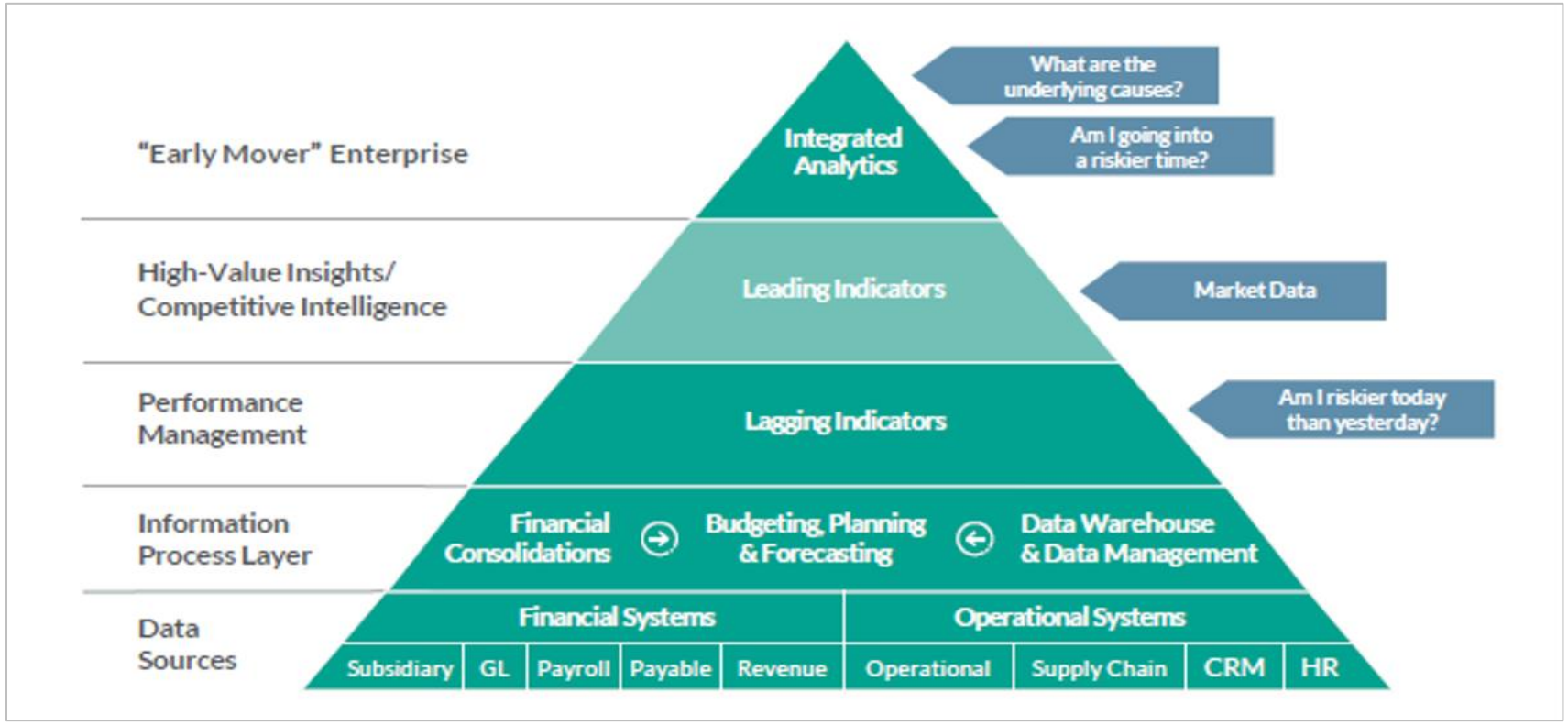
- The document does not replace the 2013 *Internal Control – Integrated Framework*
- The two frameworks are distinct and complementary
- Both use a components and principles structure
- Aspects of internal control common to enterprise risk management are not repeated
- Some aspects of internal control are developed further in this framework

Position the organization as an early mover

RECOGNIZES opportunities and risks, quickly discerning which ones are most critical	• Understands critical strategic assumptions • Applies contrarian, scenario-analysis capabilities • Conducts competitive intelligence capabilities with early alert mechanisms • Distills information in a timely manner
REACTS to opportunities and warning signs to position the organization early in the game	• Fosters a culture that is sensitive to changing market realities • Stimulates managerial intuition and ingenuity • Manages the bias, short-termism and emotional investment that can create potentially lethal organizational "blind spots"
REFLECTS on experiences to ensure continuous learning	• Encourages admission of errors and misses, and learns from them • Internalizes and converts lessons learned into improvements

When your fundamentals change, which side of the change curve will you be on? Time advantage enables proactive opportunity pursuit and risk responses.

Address the challenges of risk reporting

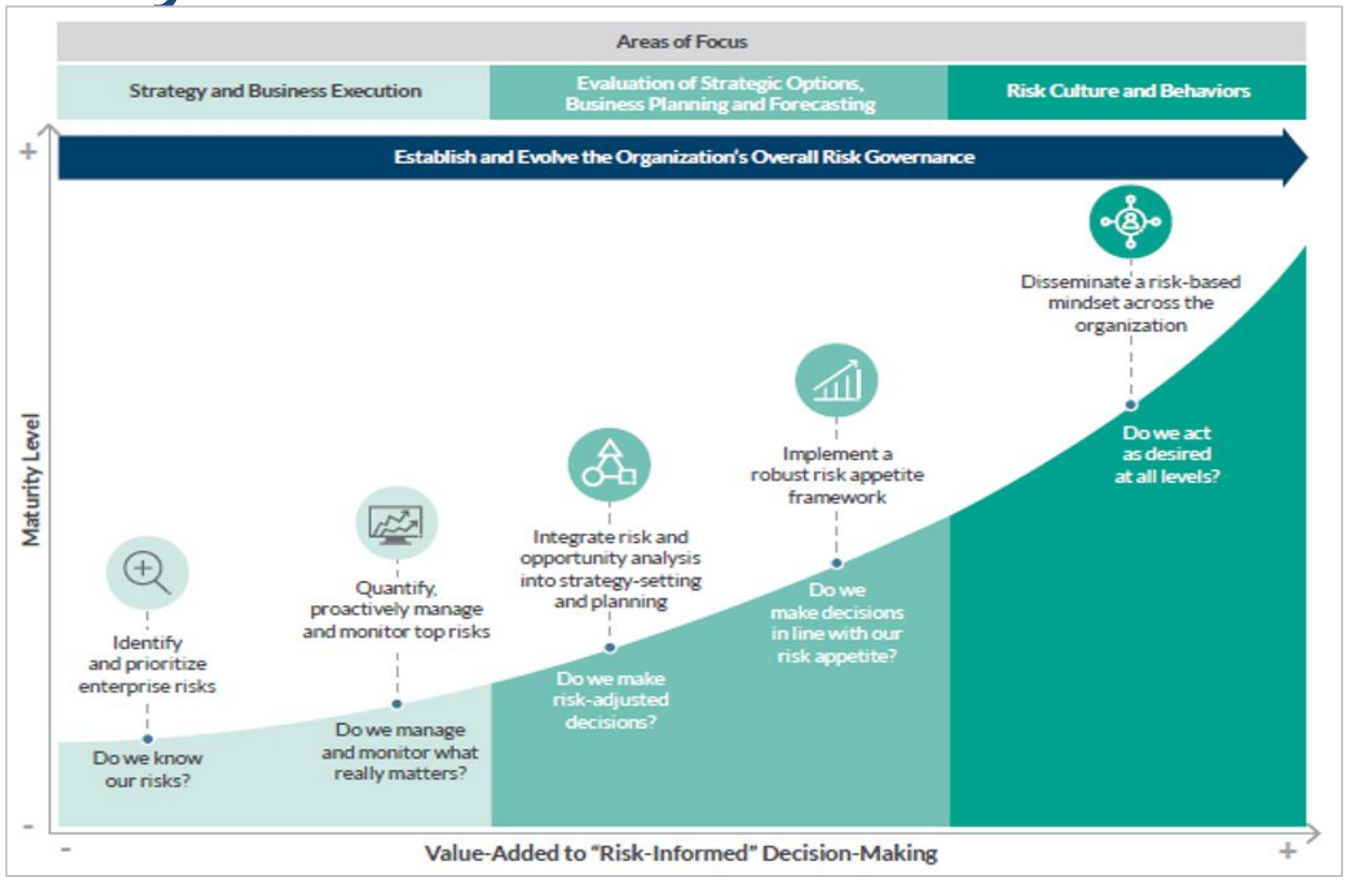


For most organizations, today's risk reporting falls short of helping companies becoming more agile and nimble in responding to a changing business environment

Protect reputation via strong lines of defense

Lines of defense offer a powerful line of sight for companies seeking to strike the appropriate balance between creating and protecting enterprise value and avoiding irresponsible business behavior

Where does management want to be on the ERM journey continuum?



- ERM is a journey
- There is no one-size-fits-all approach to implementing ERM
- The five options on the continuum are intended to be illustrative
- The four themes remain an imperative

Impact on Audit Planning

- For annual and periodic planning, internal auditors must understand:
  - The organization's business objectives and strategies
  - The risks to those objectives, and how those risks are managed
  - The organization's risk culture and risk appetite
  - The approach to review and revision

Impact on Audit Projects

- Understand which business objectives an audit may pertain to
- Align individual audit risk assessment to the organizations risk assessment
- Design scope and testing based on risk tolerance
- Report deficiencies in the context of impact on objectives

Internal Audit's Role in ERM

- Educate and facilitate understanding of ERM components and principles
- Advise and provide input to enterprise risk assessment
- Assess effectiveness of information, communication, and reporting
- Evaluate the overall effectiveness of ERM

Business and operating environments are becoming more complex and global in scale

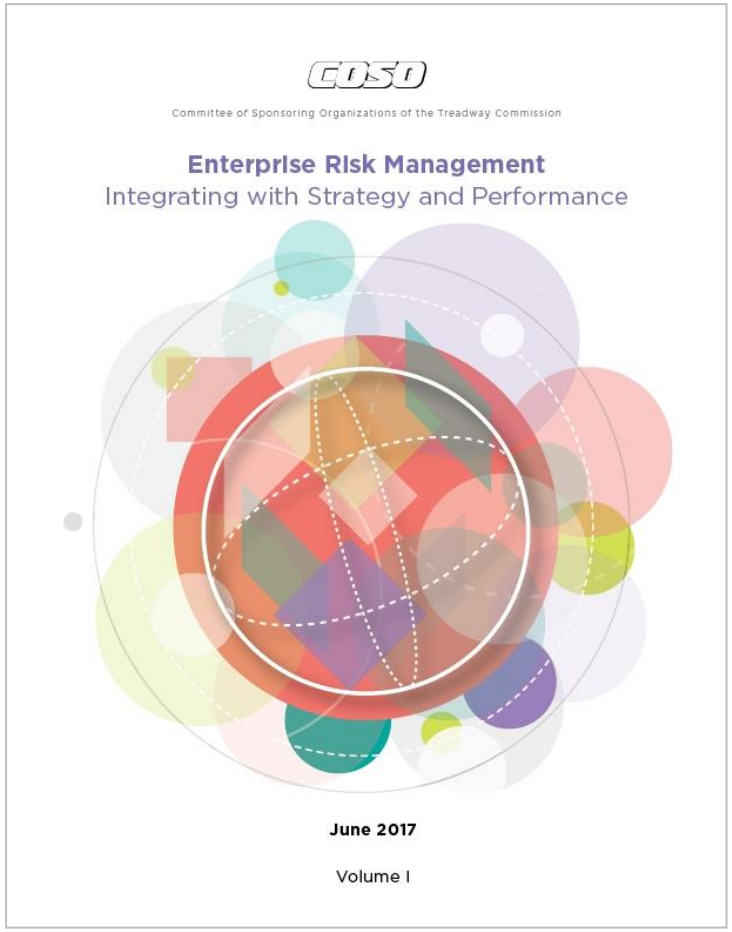
	2008	2013	2018
Top 5 Global Risks: likelihood	Asset price collapse	Severe income disparity	Extreme weather events
	Middle East instability	Chronic fiscal imbalances	Natural disasters
	Failed and failing states	Rising greenhouse gas emissions	Cyberattacks
	Oil and gas price spike	Water supply crises	Data fraud or theft
	Chronic disease, developed world	Mismanagement of population ageing	Failure of climate-change mitigation and adaptation
Top 5 Global Risks: impact	Asset price collapse	Major systemic financial failure	Weapons of mass destruction
	Retrenchment from globalization (developed)	Water supply crises	Extreme weather events
	Slowing Chinese economy (<6%)	Chronic fiscal imbalances	Natural disasters
	Oil and gas price spike	Diffusion of weapons of mass destruction	Failure of climate-change mitigation and adaptation
	Pandemics	Failure of climate-change mitigation and adaptation	Water crises

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

Applying ERM to ESG-related risks

- COSO ERM Framework principles

Thank You!


COSO
Committee of Sponsoring Organizations of the Treadway Commission
Enterprise Risk Management
Integrating with Strategy and Performance
June 2017
Volume I