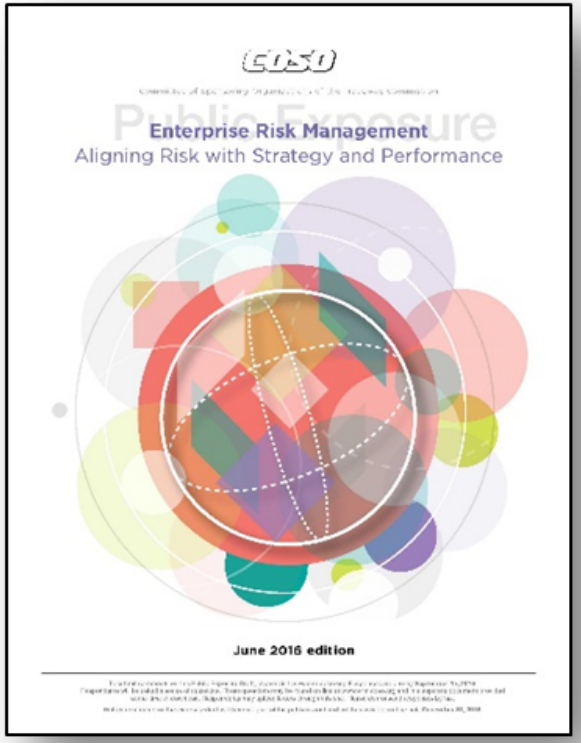
AFERM
Association for Federal Enterprise Risk Management

Enterprise Risk Management – *Aligning Risk with Strategy and Performance*

Public Exposure Draft and Comment Period June 15-September 30



Robert Hirth

COSO Chairman


KEEP
CALM
IT'S HERE!

YOU CAN HAVE THE SLIDES !!!!!!!!!!!!!!!!!!!!!!!!!!

COSO: Thought Leadership to Improve Your Organization

COSO is Happy !

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Recent “Situations”

Volkswagen

CONTROL ENVIRONMENT IS VITAL

The control environment is vital to preserving an organizations reputation and brand image.

- Since the release of the COSO Framework, there have been a number of corporate scandals related to operational compliance and reporting issues.
- Companies, besieged by persistent negative headlines, likely lacked a strong control environment in the areas that contributed to the crisis.

FOUNDATION FOR STRONG CULTURE

Control Environment

Lays the foundation for a strong culture around the organization's internal control system.

Consists of the policies, standards, processes and structures that provide the basis for effective internal control.

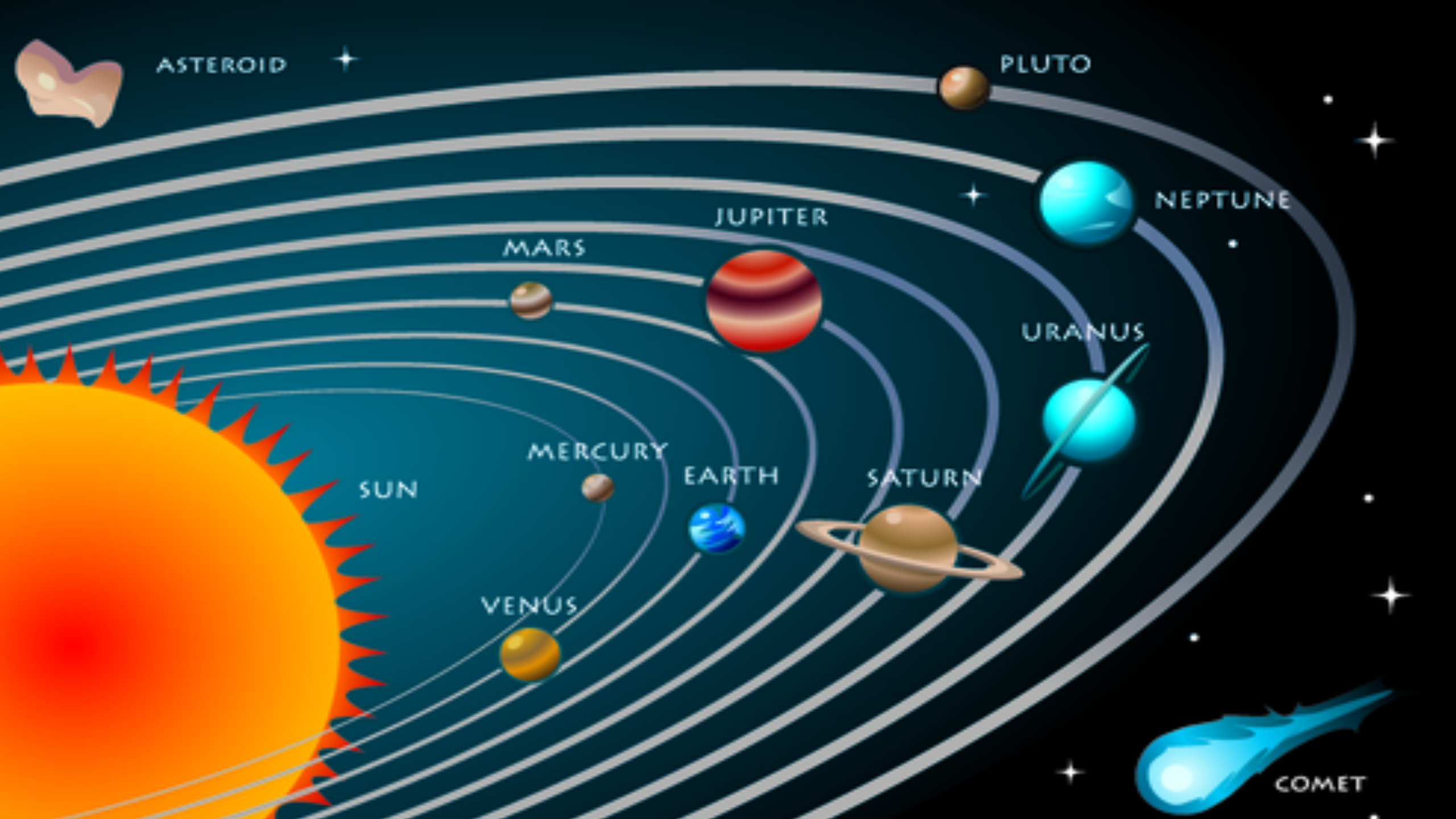
Board of directors and senior management establish the "tone at the top."

Management reinforces expectations in the organization to ensure alignment of the "tone in the middle" with the "tone at the top."

CONTROL ENVIRONMENT COMPONENTS

According to the COSO Framework, the control environment comprises the:

- **Organization's commitment to integrity and ethical values.**
- **Oversight provided by the board of directors in carrying out its governance responsibilities.**
- **Organizational structure and assignment of authority/responsibility.**
- **Process for attracting, developing and retaining competent people.**
- **Rigor around the performance measures, incentives and rewards to drive accountability for performance.**


ASTEROID
PLUTO
NEPTUNE
JUPITER
MARS
URANUS
MERCURY
SUN
EARTH
SATURN
VENUS
COMET

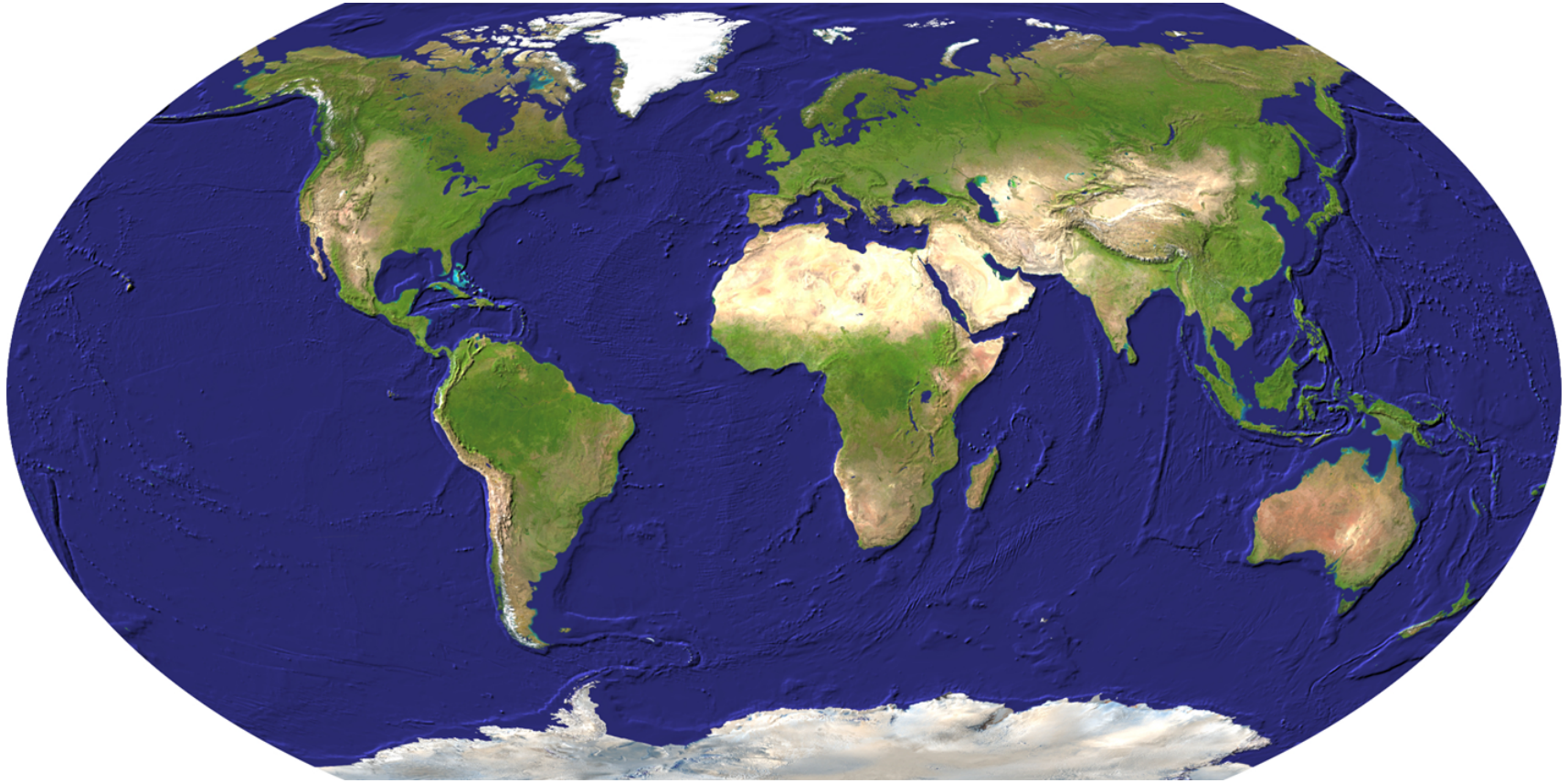
COSO Announces Project to Update *Enterprise Risk Management- Integrated Framework…*

- **NEW YORK, October 21, 2014** -- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) today announced a project to review and update the 2004 *Enterprise Risk Management–Integrated Framework* (Framework).
- The Framework, originally published in 2004, is a widely accepted framework used by management to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as it strives to increase stakeholder value.
- This initiative is intended to enhance the Framework's content and relevance in an increasingly complex business environment **so that organizations worldwide can attain better value from their enterprise risk management programs.** The initiative also will develop tools to assist management in reporting risk information and in reviewing and assessing the application of enterprise risk management.

Why Update the Framework Now?

- 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

Global Interest and Application Has Increased Significantly !



SEC Proxy Requirement…

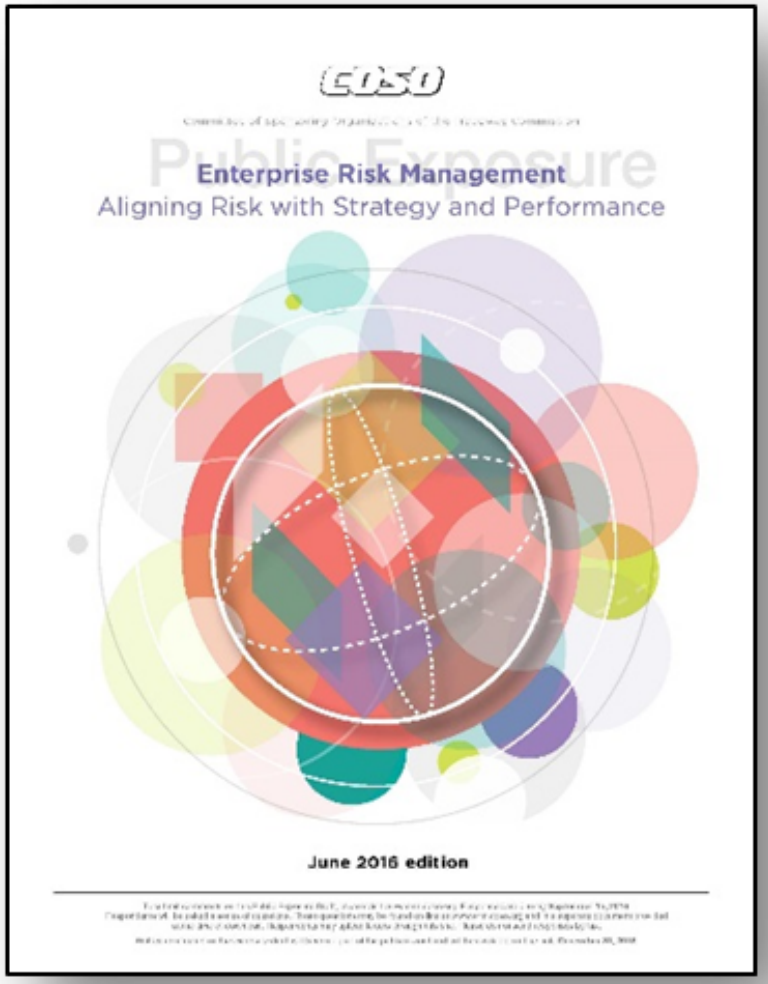
Provide Information About Board Leadership Structure and the Board's Role in Risk Oversight:

- The SEC approved rules relating to board leadership structure and the board's role in risk oversight. The rules require disclosure about:
- A company's board leadership structure, including whether the company has combined or separated the chief executive officer and chairman position, and why the company believes its structure is the most appropriate for the company at the time of the filing.
- In certain circumstances, whether and why a company has a lead independent director and the specific role of such director.
- **The extent of the board's role in the risk oversight of the company.**

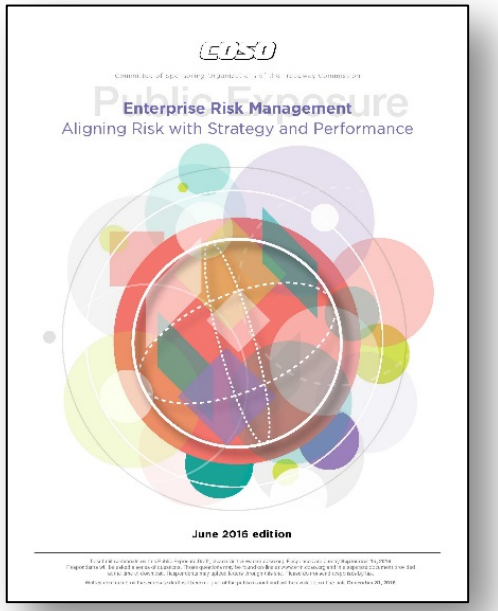
TEN PRINCIPLES OF RISK OVERSIGHT

1. Understanding the company's key drivers of success
2. Assess the risk inherent in the strategy
3. Define the role of the full board and its standing committees with regard to risk oversight
4. Consider whether the risk management system is appropriate and sufficiently resourced
5. Understand and agree with management the types and format of risk information required
6. Encourage dynamic, constructive risk dialogue between management and the board
7. Closely monitor the potential risks in the company's culture and its incentive structure
8. Monitor critical alignments – of strategy, risk, controls compliance incentives and people
9. Consider emerging and interrelated risks: What's around the next corner?
10. Periodically assess the risk oversight process in view of the board's oversight objectives

Cover Story…


COSO
Public Exposure
Enterprise Risk Management
Aligning Risk with Strategy and Performance
June 2016 edition

Why Change the Title of the Framework?



- Retitles the framework as *Enterprise Risk Management—Aligning Risk with Strategy and Performance*
- Recognizes the importance of strategy and entity performance
- Delineates between internal control and enterprise risk management
- Integrates enterprise risk management with decision making

The Strategic Value of Enterprise Risk Management

- Increases the range of opportunities
- Identifies and manages entity-wide risks
- Reduces surprises and losses
- Reduces performance variability
- Improves resource deployment
- Anticipates, identifies, adapts, and responds to change

A Key Introduction…

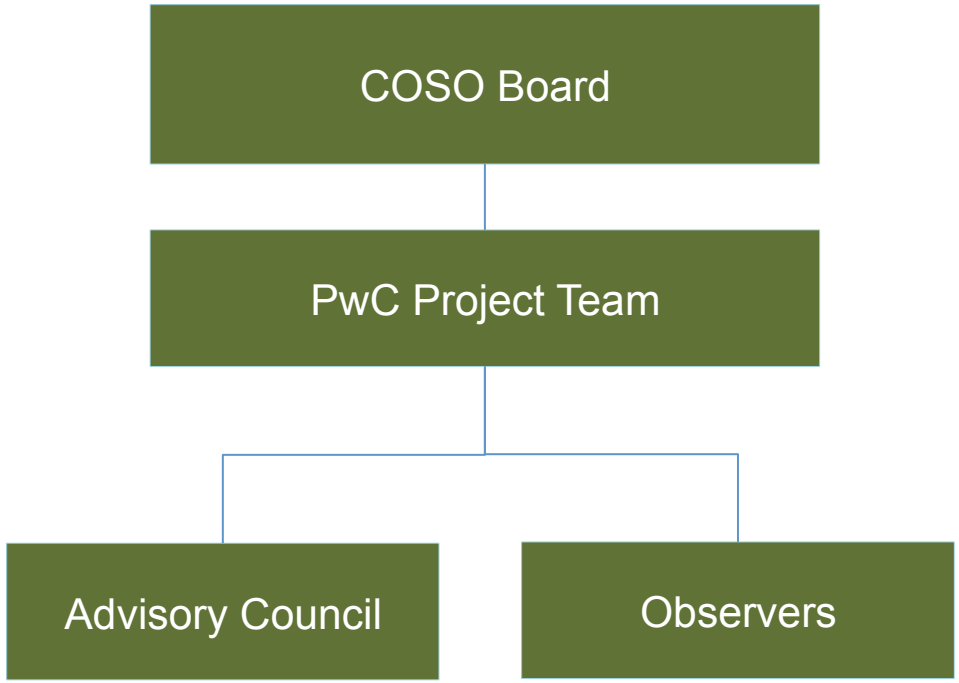
- Our understanding of the nature of risk, **the art and science of choice** lies at the core of our modern market economy.
- Every choice we make in the pursuit of objectives has its risks. From day-to-day operational decisions to the fundamental trade-offs in the boardroom, **dealing with uncertainly in these choices is a part of our organizational lives**.

The Project Update Goals

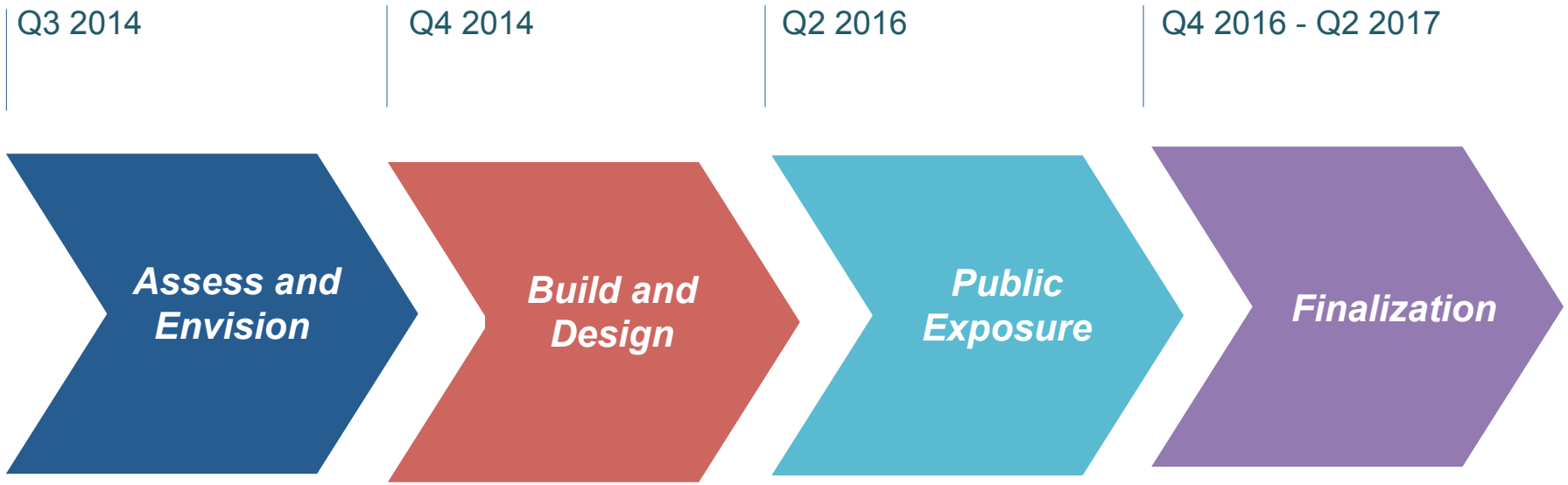
- Provide insight into strategy and the role of ERM when setting and executing strategy
- Enhance alignment between performance and ERM
- Accommodate expectation for governance and oversight
- Recognize globalization and need to apply a common albeit tailored approach
- Present new ways to view risk in setting and achieving objectives in the context of greater complexity
- Expand reporting to address greater transparency
- Accommodate evolving technology

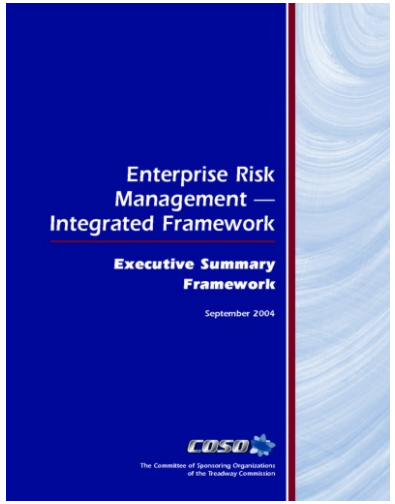
Project Governance

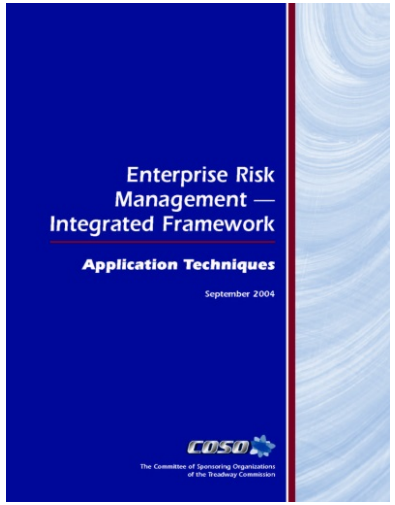
- The Advisory Council is comprised of senior executives, academics and professional risk practitioners
- Observers include representatives from regulators and industry associations



ERM Update Approach and Timing





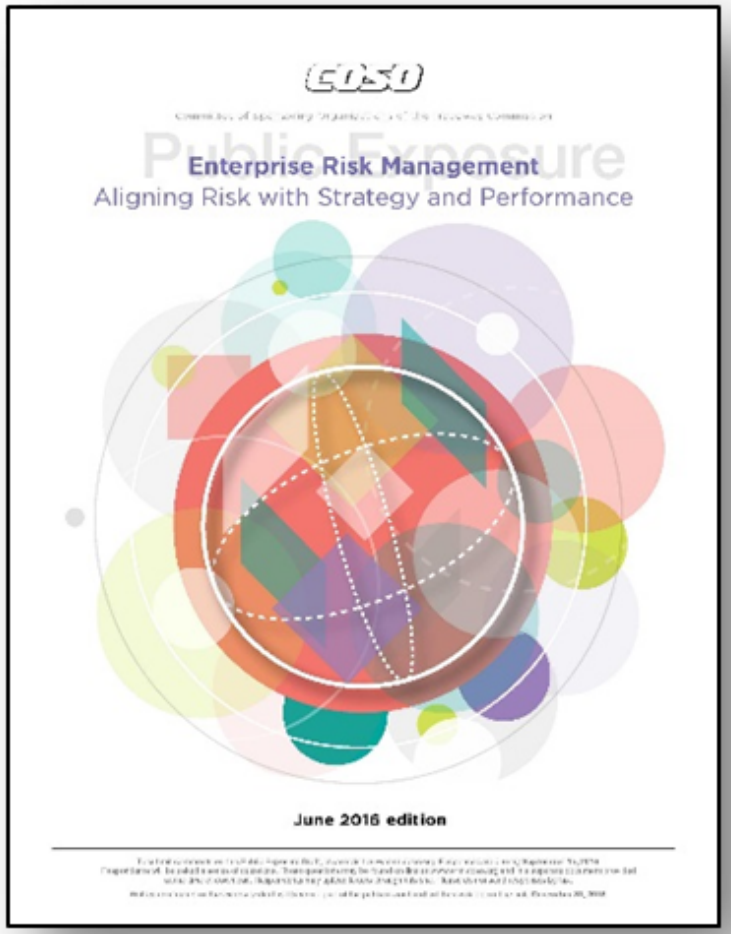


What is Being Updated

- Revises the 2004 *Enterprise Risk Management–Integrated Framework*
- Includes both the core *Framework* and related *Executive Summary*
- The *Application Techniques* volume is not being updated
- Additional thought leadership will be considered by COSO in the future

What's Available Now…

- Executive Summary
- FAQ document
- Draft Framework
- Numerous articles
- Accounting/Consulting Firm publications



Top Changes to the Framework

- ***Updates*** components and ***adopts*** principles
- ***Simplifies*** definitions
- ***Emphasizes*** value
- ***Renews*** the focus on integration
- ***Examines*** role of culture

Top Changes to the Framework, continued

- ***Elevates*** discussion of strategy
- ***Enhances*** alignment with performance
- ***Links*** with decision making
- ***Delineates*** enterprise risk management from internal control
- ***Refines*** risk appetite and acceptable variation in performance

1. Updates Components and Adopts Principles

1. Updates Components and Adopts Principles

Risk Governance and Culture

1. Exercises Board Risk Oversight
2. Establishes Governance and Operating Model
3. Defines Desired Organizational Behaviors
4. Demonstrates Commitment to Integrity and Ethics
5. Enforces Accountability
6. Attracts, Develops, and Retains Talented Individuals

Risk, Strategy, and Objective-Setting

7. Considers Risk and Business Context
8. Defines Risk Appetite
9. Evaluates Alternative Strategies
10. Considers Risk while Establishing Business Objectives
11. Defines Acceptable Variation in Performance

Risk in Execution

12. Identifies Risk in Execution
13. Assesses Severity of Risk
14. Prioritizes Risks
15. Identifies and Selects Risk Responses
16. Assesses Risk in Execution
17. Develops Portfolio View

Risk Information, Communication, and Reporting

18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance

Monitoring Enterprise Risk Management Performance

22. Monitors Substantial Change
23. Monitors Enterprise Risk Management

2. Simplifies Definitions

Risk	The possibility that events will occur and affect the achievement of strategy and business objectives (or will not occur)
Enterprise Risk Management	The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value

3. 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

4. Renews the Focus on Integration

- Integrates enterprise risk management with other business processes:

- Focuses on applying enterprise risk management at various levels of the organization (e.g. entity level, business unit, division)

5. Examines the Role of Culture

- Addresses the growing focus, attention and importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores the relationship with culture in the context of:
  - Risk governance
  - Oversight of the entity
  - Connection between framework Components
- Depicts the behavior within a risk spectrum from risk averse to risk aggressive
- Affects the entity's decision making
- Explores the alignment of culture between individual and entity behavior

6. Elevates Discussion of Strategy

- Explores enterprise risk management and 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. Enhances Alignment with Performance

- Enables the achievement of business objectives 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 acceptable variations in performance
- Manages risk in the **context of achieving business objectives** not as individual risks
- Seeks to **enhance the integrated reporting on risk and performance**

7. Enhances Alignment with Performance, continued

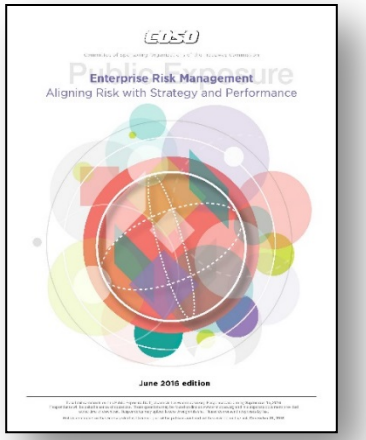
- Introduces a new depiction referred to as a risk profile
- Incorporates:
  - **Risk**
  - **Performance**
  - **Risk appetite**
  - **Risk capacity**
- Offers a dynamic and comprehensive view of risk and enables more risk-aware decision making
- The framework provides a complete depiction of how to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

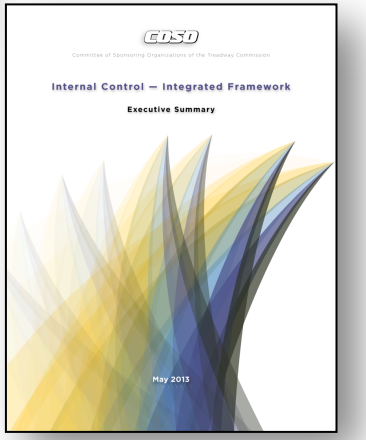
Illustrative Risk Profile

8. Links into 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

9. Delineates Between Enterprise Risk Management and 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

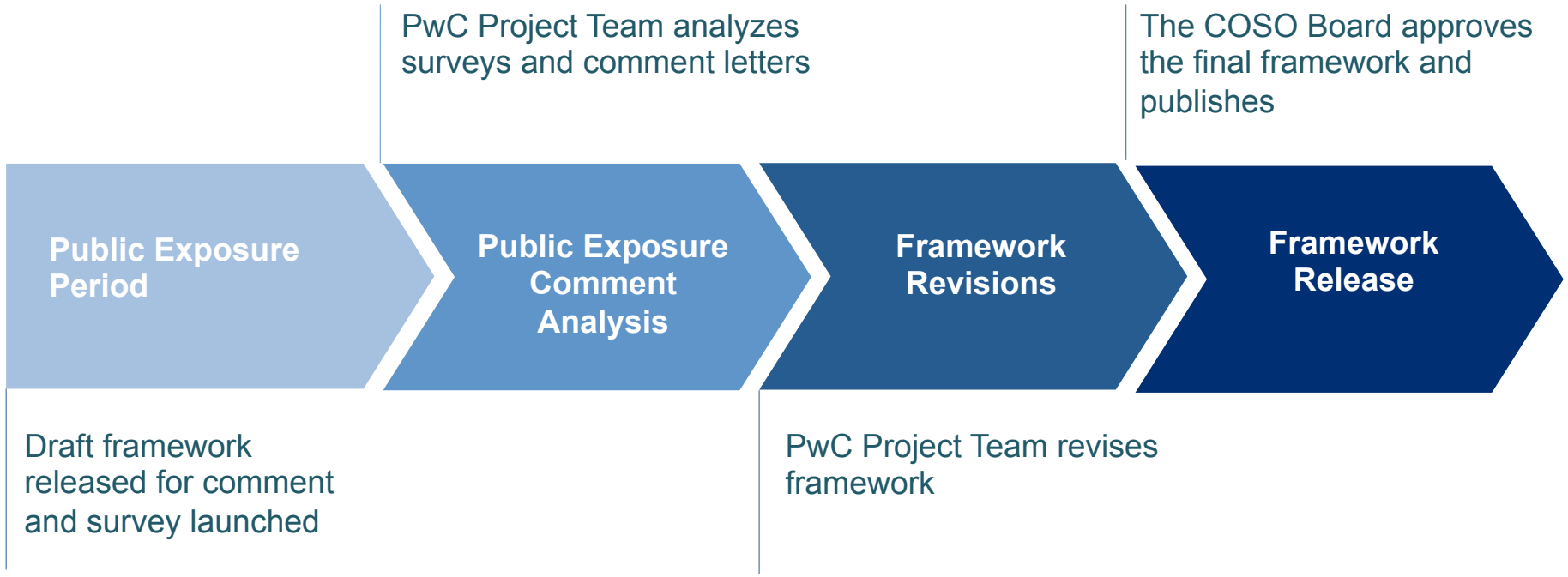
10. Refines Risk Appetite and Acceptable Variation in Performance

Risk Appetite	The amount of risk, on a broad level, an organization is willing to accept in pursuit of value
Acceptable Variation in Performance	The boundaries of acceptable outcomes related to achieving business objectives

Public Exposure Period

- Allows for the development of awareness and acceptance by the public
- Provides the ability to gain input across:
  - Geography
  - Industry
  - Risk disciplines
- Extends from June 15, 2016 through September 30, 2016 and includes:
  - Executive Summary
  - Framework
  - Appendices

Timeline of Public Exposure Period Activities



Comment Letters and Survey Responses

- 48 formal comment letters received and available for review
- Over 9,000 people commented via the structured survey
- Significant outreach via the Media and large conferences
- Smaller discussion sessions with major organizations
- Over 30,000 visits to the exposure draft site

NOW THE THOUGHTFUL WORK BEGINS !

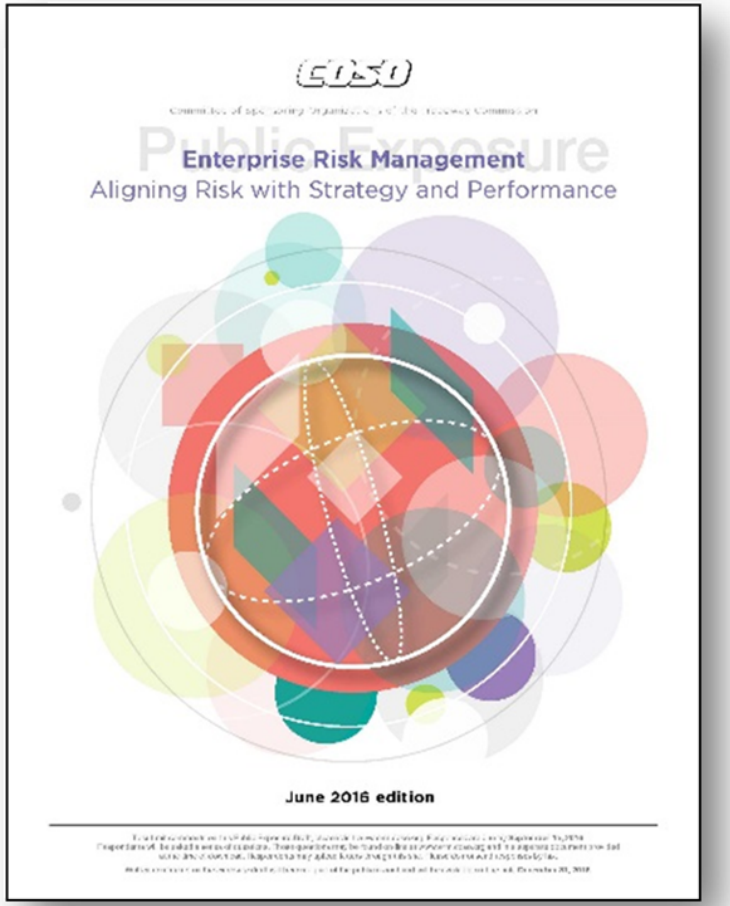
COSO Can Help ALL Organizations!

A Suitable Model Everywhere…

Incrementalism…

"How would you like to meet more of your objectives more of the time? "

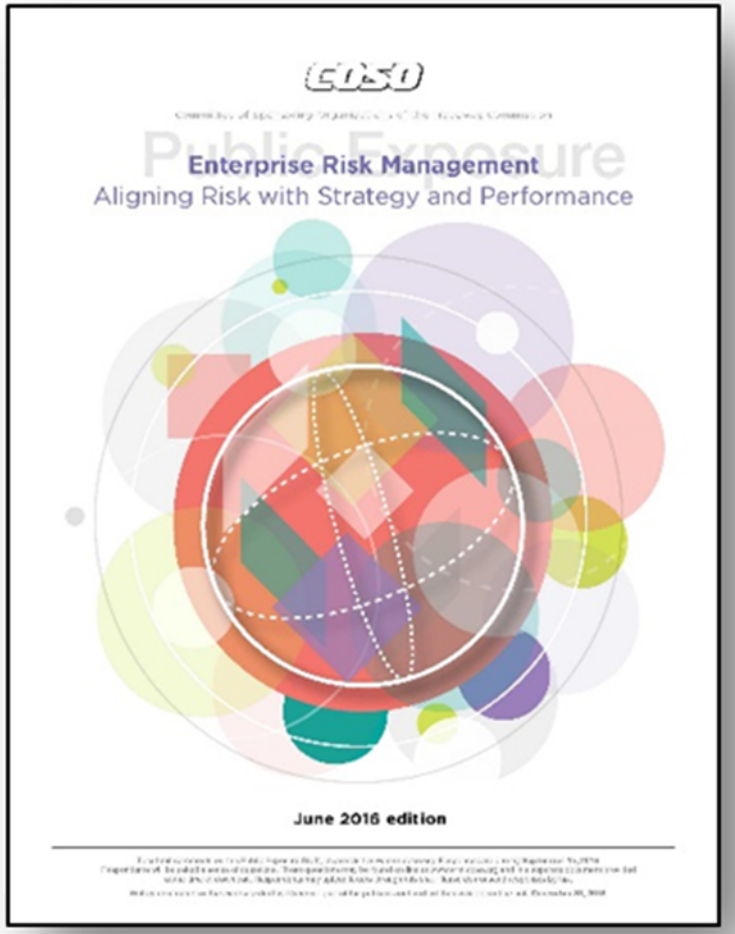
It's all About Performance …



Questions?


COSO
Public Exposure
Enterprise Risk Management
Aligning Risk with Strategy and Performance
June 2016 edition

Thank You !


COSO
Public Exposure
Enterprise Risk Management
Aligning Risk with Strategy and Performance
June 2016 edition