Enterprise Risk Management
Integrating with Strategy and Performance

Dr. Sandra B. Richtermeyer, PhD, CPA, CMA
COSO Board Member
Dean of the Manning School of Business
University of Massachusetts Lowell - USA
New ERM Framework – Focus on *Integration*
Two COSO Frameworks

- Internal Control Integrated Framework
- Enterprise Risk Management Framework

Both focus on

- Thought leadership
- Organizational improvement
Integrity and Ethical Values are CRITICAL

- Consistent with most organizational **values**
- Fundamental to our **culture**, interactions
- Integral to **professionalism** as a person
- Integral to accounting profession as an expected **core behavior**
- Provides **confidence** in you by others
- **Foundational** to COSO
- **Accountability** is a consequence
- **NOT EASY**
Cover Story…
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?

- 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
Key takeaway from ERM update process - global interest and application have increased significantly!
U.S. Securities & Exchange Commission (SEC) Proxy Requirement…

*Boards are required to disclose items related to 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.
Why a title change?

- Retitles the framework with integration as a key feature
- 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 uncertainty 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 but 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

Q3 2014 - Assess and Envision
Q4 2014 - Build and Design
Q2 2016 - Public Exposure
Q4 2016 - Q2 2017 - Finalization
What is Included in Update?

- 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 is 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
2. Simplifies Definitions

<table>
<thead>
<tr>
<th>Risk</th>
<th>The possibility that events will occur and affect the achievement of strategy and business objectives (or will not occur).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise Risk Management</td>
<td>The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value.</td>
</tr>
</tbody>
</table>
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
- Dynamic and comprehensive view of risk
- Enables more risk-aware decision making
- 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
Incrementalism…

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

- Allowed for the development of awareness and acceptance by the public
- Provides the ability to gain input across:
  - Geography
  - Industry
  - Risk disciplines
- Included Executive Summary, Framework & Appendices
Public Comments

• Integral to the COSO framework revision process
• Enhances confidence by regulators
• Leverages other good thinking
• Provides non-US perspective
• Challenges our assumptions
• Provides confirmation
• Creates improvement
Summary of Public Exposure Feedback

- Over 200 survey responses – double that of the *Internal Control-Integrated Framework* update
- Over 70% of responses from individuals, who are often less inclined to write letters
- Over 50% of participation outside of North America
- Almost 50% of those responding had affiliations beyond COSO memberships
- Almost 50% of respondents had 10 or more years of risk management experience
- Positive ratings outnumbered negative ratings by 4.5:1

- 48 letters received – many of which demonstrated considerable investment
- Comments on concepts (flawed missing, unnecessary) collectively represented less than 15% of the total number of comments received
- Greatest number of comments requested clarity of drafted content versus adding/deleting content
Downloads of the updated Framework

- Almost 10,000 downloads of the document during the public exposure period
- Strong international interest in the Update, with 46% of the downloads occurring outside North America
- Widespread interest across industries
- Proportional interest between private and public companies
- Risk management and internal audit roles combined to represent 40% of total downloads

Feedback to the PwC Project Team

Four channels for capturing input represented the most diverse approach undertaken for any COSO project, consisting of:

- **Survey** feedback provided through the website
- **Letters** provided by associations, companies, and individuals
- **Meetings, Conferences, Seminars** attended by the PwC Project Team, providing direct feedback on the update
- **Social Media** outreach with over 3 million connections
Key Areas of Feedback Related to:

- Culture
- Decision-making
- Definitions
- Integration of ERM
- Risk assessment
- Risk information
- Strategy
Timeline of Public Exposure Period Activities

- **Public Exposure Period**: Draft framework released for comment and survey launched
- **Public Exposure Comment Analysis**: PwC Project Team analyzes surveys and comment letters
- **Framework Revisions**: PwC Project Team revises framework
- **Framework Release**: The COSO Board approves the final framework and publishes
What Might Change…

- # of Principles
- Graphics
- Linkage to internal control
- Definitions
- Change “Execution”
- More integration explanation
- “Wordsmithing”
What’s Not Likely to Change…

- Integration with strategy setting
- Board oversight
- Link to performance
- Use in decision-making
- Components and principles structure
- Risk profiles concept
- “DNA” embedded- not a function
- Examples compendium (not in public comment)
COSO Can Help ALL Organizations!
A Suitable Model Everywhere…
It’s All About Performance …