COSO Enterprise Risk Management – Integrating with Strategy and Performance

AFERM Summit
November, 2017
**Agenda**

1. Introducing COSO
2. Why update the Framework now?
3. What has changed?
4. What does it mean for you?
5. More information

*COSO recognizes the growing expectation of organizations to manage, in an integrated and cohesive manner, risks emanating from across an enterprise.*

Robert B. Hirth Jr., COSO Chair
Introducing COSO
Updating one of the world’s most widely used risk management frameworks

2004 Publication

2017 Publication

Other COSO publications
What prompted the Framework update?
What are risk and business professionals saying?

As an innovative company, I want to use risk to create value and not only to protect value.

I want to reduce performance variability and respond more quickly to opportunities.

I need insights that help me understand risks and opportunities and evaluate strategic options.

When I develop my strategy, I want to have a full picture of the potential risks and the capabilities I need to create advantage.

I want an ERM Framework that drives improvements to business functions beyond risk avoidance.

COSO Enterprise Risk Management Framework - Integrating with Strategy and Performance
Why update the ERM framework now?

- **Boards are expecting more** from their organization’s ERM practices and capabilities
- Stakeholders are seeking **greater transparency** and accountability
- 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**

Since 2004, the market has continued to evolve and the COSO Framework is evolving with it.
What’s changed?
Introducing the 10 key changes to the 2017 Framework

- A new framework structure
- A focus on integrating risk management
- Written from the perspective of the business
- Explores management of risk at all altitudes of the organization
- Greater emphasis on culture
- Explores the different benefits of ERM
- Suite of new graphics highlighting the relationship between risk and performance
- Deeper discussions on challenging topics
- Addresses the evolving role of technology
- Coming soon: Compendium of Example
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.
The new Framework adopts a components and principles structure

COSO Enterprise Risk Management Framework - Integrating with Strategy and Performance
### Explores the benefits of ERM

- Enterprise risk management frameworks are as varied as the organizations they support.
- In their infancy, many frameworks focus on reducing negative surprises and identifying entity-wide risks.
- Boards, senior management and stakeholders are increasingly expecting ERM to go further to deliver greater benefits.

**ERM Benefits**
- Reducing negative outcomes
- Enhancing enterprise resilience
- Improving resource deployment
- Identifying and managing risks entity-wide
- Increasing the range of opportunities
- Reducing performance variability
Question 1:

During the development of the ERM Framework, we heard repeated calls for a closer link with risk and strategy. Do you feel:

a) it is time to get risk at the strategic planning table

b) many are still trying to find their way in this conversation

c) this is a wasted effort and nothing will change at the strategy level
Focusing on integrating risk and strategy

81% of the greatest losses in shareholder value since 2002 were attributable to ‘strategic blunders’

- 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

*U.S. public companies around the world with at least US$1 billion in enterprise value on January 1, 2002 (1,053 companies met these criteria). Dann, Le Merle and Pencavel, “The Lesson in Lost Value” Strategy+Business, November, 2012
Focusing on integrating risk and strategy

The updated Framework elevates the discussion of 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
Question 2:

We've been getting lots of input about the need to bring risk considerations into decision-making. Would you say that is:

a) a widely held view

b) necessary but far from reality

c) a voice from the louder minority
New graphics depict the alignment between risk and performance

Questions for your organization

Is the risk assumed by the entity, when setting performance targets, understood?

What assumptions inform the shape of the risk curve?

Do existing key indicators demonstrate movement along the curve?

What level of performance is assumed when assessing impact and likelihood?

Business objective: Increase sales

Amount of Risk

Acceptable Variation

Performance Target

Number of Units Sold

Risk Curve

Risk Appetite

Where on the curve should ERM focus?
Explores managing risk at all altitudes of the organization

The Framework highlights that **risks emanate and must be managed at all levels** of the organization.

The Framework also addresses how **risks can change in severity and prioritization at different levels** of the organization.
Written from the perspective of the business

The framework was written from the perspective of the business to facilitate the integration of ERM

- Research has confirmed that there is often a ‘siloed’ or incremental approach to risk management that is separate from the day to day management of an organization

- The lack of integration can contribute to difficulties engaging with the business, the ability to gain and offer insight and ultimately curbs the value that ERM can offer

- The Framework endeavors to remove risk ‘jargon’ and adopts the language of business to discuss concepts and practices
How the Framework addresses culture

Culture now features in the definition of ERM and is part of the Framework’s Governance and Culture Component.

Principles on culture are now 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.

Discussions on the importance and commitment to integrity and ethics have been retained in the COSO Internal Control Integrated Framework.
A compendium of examples is also being developed. The proposed compendium will illustrate:

- All principles
- A variety of entity sizes from global through to national, regional, and local entities
- A variety of industry types
- Actual company practices and be augmented with expected practices in select areas, as needed
- Written from the perspective of the business
What does this mean for you and your organization?
Question 3:

Where do you see yourself choosing to focus with regards to the Framework’s adoption?

- a) risk's relevance to strategy
- b) risks relationship to performance
- c) culture's consideration of risk
- d) I have no idea or don’t plan to do anything with my program
Where to next?

Encourage your risk professionals to:
- Sync with the language of business in your organization
- Understand how organization creates, realizes and preserves value and the supporting assumptions
- Develop a clear understanding of where ERM is integrated

Challenge your organization to not:
- View ERM simply as a function, team or department
- Consider ERM to be a stand alone, periodic risk assessment or heat map
- View GRC technology as the entire approach for implementing ERM
More information
Staying involved

Access the Framework at www.coso.org
Thank you