COSO Enterprise risk management – Aligning risk with strategy & performance

IIA Winnipeg

May 2, 2017
Agenda

1 Why Update the Enterprise Risk Management Framework Now

2 Depicting and Clarifying Enterprise Risk Management

3 What’s Changed

4 Overview of Feedback Received during Public Comment

5 COSO Compendium of Examples

6 Staying Involved
COSO’s 2004 Enterprise Risk Management – Integrated Framework is one of the world’s most widely used risk management frameworks.

www.coso.org

COSO and PwC have collaborated on frameworks and publications for 25 years

2004

2017 Publication

Other COSO publications authored by PwC
Why update the ERM framework now?

Since 2004, the market has continued to evolve and the COSO Framework is evolving with it.

- ERM concepts and **practices have evolved** and the bar is rising
- There is a need to **incorporate lessons learned** from recent events
- Business **environments are increasingly complex**, technologically driven, and global in scale
- Stakeholders are seeking **greater transparency** and accountability
- Risk **discussions are increasingly prominent** at the board level
Depicting Enterprise Risk Management

The updated Framework includes a new graphic to illustrate the alignment of risk, strategy, and performance

2004 COSO ERM graphic

Updated COSO ERM Graphic


COSO Enterprise Risk Management: Aligning Risk with Strategy and Performance
Public Exposure Draft (2016)
Clarifying Enterprise Risk Management

Similar to recent COSO Frameworks and guidance, the updated Framework sets out a series of principles

These principles:

• Depict the essential aspects of enterprise risk management
• Apply to organizations of all legal structures, size, and purpose
• Are not specific rules that replace management judgment

Clarifying Enterprise Risk Management (continued)

What’s changed since 2004

In addition to a new title, the more substantive changes related to:

1. **Strategy**
   - Elevates discussion of strategy

2. **Performance**
   - Enhances alignment between performance and enterprise risk management

3. **Culture**
   - Examines the role of culture

4. **Controls**
   - Delineates between enterprise risk management and internal controls
What our research is telling us...

Companies where ‘strategic blunders’ resulted in the greatest losses of shareholder value since 2002*

81%

*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
Elevates discussion of risk and strategy

- Research suggests that organizations are looking to strengthen the integration between strategy and enterprise risk management.
- Consider where do your ERM efforts currently focus and how closely does it align to value creation, realization and preservation?

Enhances alignment between risk and performance

The Framework considers how risk relates to performance

For instance, it explores the questions:

- Does the entity understand the risk it is taking when setting performance targets?
- Has the entity performed as expected and achieved its target?
- What risks are occurring that may be affecting performance?
- Did the entity take enough risk to attain its target?

ERM practices focus on the potential for risk to impact strategy and objectives and the relationship to overall performance.
Examines roles of risk culture

- The Framework sets out a “culture spectrum” which aligns with the conversation on risk appetite.
- Measuring and reporting on culture remain a key challenge and will likely evolve significantly in the coming years.

Risk culture is linked to the conversation of management’s attitude towards risk taking.

<table>
<thead>
<tr>
<th>Risk appetite</th>
<th>Lower</th>
<th>Higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Culture</td>
<td>Risk Averse</td>
<td>Risk Neutral</td>
</tr>
</tbody>
</table>
Delineates relationship between ERM and internal controls

- Internal control remains an integral part of ERM, although users are looking for a more focused ERM document

- Aspects of internal control that are common to both this publication and COSO Internal Control – *Integrated Framework are not repeated* in the updated Framework

- Where necessary, aspects of internal control are further developed in the updated Framework

- The two COSO Frameworks are distinct and provide a different focus – neither supersedes the other
Channels of input to PwC project team

1 Survey
Survey responses provided through the website

2 Letters
Letters provided by associations, companies, and individuals

3 Meetings, conferences
Over 40 meetings, conferences and seminars attended by the Project Team, providing direct feedback on the Update

4 Social media
Social media created over 2.8 million impressions and 3,000 direct interactions from viewers

Overall input to project team
Key highlights from the public exposure period

1. Site visits
   - Over 24,000 site visits

2. Global interest
   - 46% of the downloads outside of the US

3. Entity interest
   - Wide spread interest across industry

4. Engagement
   - Equal interest by private & public companies
### Key highlights from feedback received

<table>
<thead>
<tr>
<th>Letters &amp; surveys</th>
<th>Comments</th>
<th>Themes</th>
<th>Feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>217 surveys submitted, 47 letters received</td>
<td>2,000 individual comments</td>
<td>Encouraging breadth of comments</td>
<td>Positive ratings outnumbered negative by 4.5:1</td>
</tr>
</tbody>
</table>
Summary of public exposure feedback

- Focusing on strategy is the right way forward
- What is good ERM culture?
- Need greater emphasis on decision-making
- Suggestions for new definitions of Risk and ERM
- Explain how this differs from IC?
- Highlight importance of integration more consistently throughout the document

Comments related to...

- Strategy
- Culture
- Decision-making
- Definitions
- Integration
- Internal control
- Risk tolerance
- Risk assessment
- Risk information

- Include more discussion on Big Data and AI
- How do I draw risk curves?
- Why does the document not refer to risk tolerance?

Focusing on strategy is the right way forward

What is good ERM culture?

Need greater emphasis on decision-making

Suggestions for new definitions of Risk and ERM

Explain how this differs from IC?

Highlight importance of integration more consistently throughout the document
What’s changing?

In response to feedback received during the public comment period, the Project team intends to:

• Reduce the number of principles
• Update graphics
• Refine linkages to internal control
• Change component titles
• Increase emphasis on integration and decision-making
• Highlight culture and relationship to core values
• Expand the conversation on information and technology

A summary of changes will be outlined in the Framework
A compendium of examples is also being prepared. 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
## Where to next?

**Encourage your risk practitioners 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 organizations 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
Staying involved

Download the draft Framework at www.coso.org

Sign up for updates and view videos, blogs and articles at http://www.pwc.com/us/en/risk-management/coso-erm-framework

Frank Martens

Lead Director, COSO Project Update
Global Risk Framework and Methodology Leader
Tel: 604-806-7590
Frank.j.martens@pwc.com
ca.linkedin.com/in/frankmartens

Robert Reimer, PwC Winnipeg, Tel: 204-926-2442
Robert.j.reimer@pwc.com

Gerry Valois, PwC Winnipeg, Tel 204-926-2455
Gerry.valois@pwc.com
Thank you