Enterprise Risk Management - Aligning Risk with Strategy and Performance

November 18, 2016

weaver
Assurance • Tax • Advisory

IASA
Progress Through Sharing Knowledge
Qualifying Statement

• The comments and statements in this presentation are the opinions of the speaker and do not necessarily reflect the opinions or positions of Weaver and Tidwell, LLP. (dba Weaver).
• No part of this document may be reproduced, transmitted or otherwise distributed in any form without written permission from Weaver.
• Weaver expressly disclaims any liability in connection with the use of this presentation or its contents by any third party.
• The contents in this presentation relating to the Updated ERM Framework are in Exposure Draft at the date of this presentation, and therefore, are subject to change.
Topics

• History of ERM
• Why Update the Current Framework?
• Exposure Draft Questions
• The Updated Framework and Key Changes
• Public Responses
• COSO Releases Fraud Risk Management Guide
History of ERM
History of ERM Framework

1985: COSO is organized


1992: Internal Control – Integrated Framework is published


2004: Guidance on Monitoring Internal Control Systems is published

2006: Internal Control – Integrated Framework Reissued

2009: COSO invites public review on the revised framework Fraud Risk Management Guide issued

2010: Plan to update ERM Framework announced

2013: COSO expects to release final version of updated Enterprise Risk Management Framework

2014

2016

2017
Current ERM Framework

• **ERM is:**
  – An ongoing process
  – Effected by people
  – Applied in strategy setting
  – Applied across the company, at all levels
  – Identifies potential events within risk appetites
  – Provides assurance to management and board
  – Geared to achieving objectives
Why Update the Current Framework?
Why is an Update Needed?

Since 2004:

- **New risks** have emerged
- **Boards** are more aware and involved in risk management reporting
- **Operating environments** are more complex - technologically and global in scale
- **Stakeholders** are more engaged, seek greater transparency and accountability
The Update Process

- Enterprise Risk Management – Aligning Risk with Strategy and Performance:
  - Issued for public comment 6.15.16 and ended 9.30.16
  - Comment letters are available to the public on coso.org through 12.15.16
Exposure Draft Questions

- **Is adoption of the updated Framework mandatory?**
  - **No**, as there are different regulatory, stakeholder and industry requirements

- **Can I still use the 2004 ERM-Integrated Framework?**
  - **Yes**, though COSO reserves the right to supersede the entire 2004 Framework
Exposure Draft Questions?

• **Who is the updated Framework applicable to?**
  – **All entities**, including not-for-profit and governmental

• **Why change the title?**
  – New title recognizes importance between strategy and entity performance
Exposure Draft Questions?

- Where is the COSO cube?
  - Cube graphic is still used in the 2004 Framework
  - Updated Framework has a new graphic showing the alignment of risk, strategy and performance
The Updated Framework and Key Changes
Enterprise Risk Management - Integrated Framework

Enterprise Risk Management: Aligning Risk with Strategy and Performance

Recognizes the importance of the connection between strategy and entity performance
**Updated ERM Definition**

**Simplifies the definition of ERM:**

- To improve clarity for ERM users
- More closely aligns risk to value

---

ERM is a process, effected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The culture, capabilities, and practices, integrated with strategy and execution, that organizations rely on to manage risk in creating, preserving, and realizing value.
Changes in Structure

Adapts a Components & Principles Structure:

• From 8 components in 2004
• To 5 components in 2016 with 23 supporting principles
Updated Graphic

New Visual: Highlights the 5 components and 23 principles

Risk Information, Communication, and Reporting
Risk Governance and Culture
Risk, Strategy, and Objective-Setting
Risk in Execution
Monitoring Enterprise Risk Management Performance
Enhanced Performance
Strategy and Business Objectives
Mission, Vision, and Core Values
Components & Principles

Risk Governance and Culture

1. Exercise 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 Governance sets the entity’s tone
Culture is reflected in decision making

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

Sets Risk Appetite
Looks at what risks prevent achieving Strategy and Objectives
Components & Principles

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

- What risks **prevent** achieving strategy and objectives
- Portfolio View of risk **assumed** in **pursuing** strategy and objectives
- **IT Systems** capture, process and manage data/ information
- Information used in **reporting**
- How well is risk management **functioning**
Risk and Value

Emphasizes the Relationship Between Risk and Value:

• No longer just focused on preventing the erosion of value and reducing risk to target levels
• Now looks at the role ERM has in creating, preserving and realizing value
• Viewed as integral to strategy setting and identifying opportunities that create value
Integration with Management

Renews the Focus on Integrating ERM:

- Encourages users to integrate ERM into management rather than in a siloed activity
Looks at Culture

Examines the Role of Culture:

• Culture influences **(not in current framework)**:
  – Risk governance
  – Management and board oversight
  – Effectiveness of other Framework components

“I don’t know how it started, either. All I know is that it’s part of our corporate culture.”
Elevates the Discussion of Strategy:

- The updated Framework expands discussion of strategy and risk by focusing on three concepts:
  1. The possibility of strategy and business objectives **not aligning** with mission, vision, and values
  2. The **implications** of the strategy chosen
  3. Risk in **executing** the strategy
Enhances the Alignment Between Performance & ERM:

- Focuses on how risk is integral to setting business objectives and performance targets:
  - How ERM identifies and assesses risks impacting performance
  - How variations in performance help users understand the impact of changes to risk profile of business objectives or vice versa
  - Emphasizes risk assessments are not done to generate long lists of risks - rather highlights how risks impact strategies and objectives

"I think we need to take another look at your risk management strategy..."
Risk Concepts

• Risk Profile
  - Incorporates concepts of risk appetite, performance and risk into a single graphic offering more risk-aware decision making
Decision Making

Links ERM into Decision-Making More Explicitly:

• Explores how information about the risk profile enhances overall decision making
Internal Control

Delineates Between ERM & Internal Controls:

- Update **does not** replace the 2013 Internal Control – Integrated Framework
- Both frameworks use a structure of **components** and **principles**
- Internal control common to both frameworks are **not repeated** – such as **control activities**
- The Update **further develops** the governance aspects of ERM.
Redefining Risk Tolerance

Refines Risk Appetite & Acceptable Variation in Performance (often referred to as risk tolerance):

- Risk Tolerance defined using performance and not a more detailed version of risk appetite
- Redefining risk tolerance:
  - Amount of risk acceptable for a given performance
  - Boundaries of acceptable risk in context of performance
  - Assesses whether changing levels of performance remain within limits of acceptable variation
  - Risk and performance no longer considered separate and static entities

“Jon, betting your project budget on double zero is not a risk management plan.”
## Public Responses

<table>
<thead>
<tr>
<th>Positives</th>
<th>Negatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Recognizes the connection between risk, strategy, and performance</td>
<td>• Too long and too technical</td>
</tr>
<tr>
<td>• Emphasizes the importance of culture</td>
<td>• Definitions are not consistent through the document</td>
</tr>
<tr>
<td>• Detailed enough to guide communication with management about risk</td>
<td>• Not enough consideration is given to the positive outcomes of risk</td>
</tr>
<tr>
<td></td>
<td>• Not enough practical examples or guidance provided</td>
</tr>
<tr>
<td></td>
<td>• Doesn’t provide examples for other forms of businesses like non-profits or governments</td>
</tr>
</tbody>
</table>
**COSO Fraud Risk Management Guide (2016)**

**Fraud Risk Governance**
- Communicate the Fraud Risk Management Program reflecting expectations of board / senior management, and commitment to high integrity and ethical values for managing fraud risk

**Fraud Risk Assessment**
- Perform fraud risk assessments to identify fraud schemes and risks, assess their likelihood and significance, evaluate fraud control activities, and implement actions to mitigate residual fraud risks

**Fraud Control Activity**
- Select, develop, deploy preventative and detective fraud controls to mitigate risk of fraud events occurring or not being detected timely

**Fraud Investigation and Corrective Action**
- Establish a communication process to obtain information about potential fraud, deploy approach to investigate and implement corrective action to address fraud timely

**Fraud Risk Management and Monitoring Activities**
- Select, deploy, and perform evaluations to ascertain the five principles of fraud risk management is present and functioning. Communicate deficiencies timely to senior management and the board.