Achieving and Sustaining Success with COSO ERM

Paul J. Sobel, CIA, QIAL, CRMA
COSO Chairman
Chief Risk Officer – Georgia-Pacific LLC
Focus of Presentation

• Key Things to Know about the New Framework
• Impact on Internal Auditing
• Compendium of Examples
• Applying ERM to Specific Areas of Risk
• Potential New Guidance
A New Title…

Retitled as *Enterprise Risk Management—Integrating with Strategy and Performance*

Recognizes the importance of strategy and entity performance

Further distinguishes enterprise risk management from internal control
Incorporates New Graphics/Concepts

Graphic has stronger ties to the business model

ENTERPRISE RISK MANAGEMENT

MISSION, VISION & CORE VALUES

STRATEGY DEVELOPMENT

BUSINESS OBJECTIVE FORMULATION

IMPLEMENTATION & PERFORMANCE

ENHANCED VALUE

Governance & Culture

Strategy & Objective-Setting

Performance

Review & Revision

Information, Communication, & Reporting
## Introduces Principles

### 20 key principles within each of the five components

<table>
<thead>
<tr>
<th>Governance &amp; Culture</th>
<th>Strategy &amp; Objective-Setting</th>
<th>Performance</th>
<th>Review &amp; Revision</th>
<th>Information, Communication, &amp; Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Attracts, Develops, and Retains Capable Individuals</td>
<td></td>
<td>14. Develops Portfolio View</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
Links to Strategy

Explores 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
Recognizes Importance of Culture

- Addresses the growing focus, attention and Importance of culture within enterprise risk management
- Influences all aspects of enterprise risk management
- Explores culture within the broader context of overall core values
- Depicts culture behavior within a risk spectrum
- Explores the possible effects of culture on decision making
- Explores the alignment of culture between individual and entity behavior
Builds Links to 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
Impact on Audit Planning

• For annual and periodic planning, internal auditors must understand:
  – The organization’s business objectives and strategies
  – The risks to those objectives, and how those risks are managed
  – The organization’s risk culture and risk appetite
  – The approach to review and revision
Impact on Audit Projects

• Understand applicable business objectives for an audit
• Align individual audit risk assessment to the organizations risk assessment
• Design scope and testing based on risk tolerance
• Report deficiencies in the context of impact on objectives
Internal Audit’s Role in ERM

- Educate and facilitate understanding of ERM components and principles
- Advise and provide input to enterprise risk assessment
- Assess effectiveness of information, communication and reporting
- Evaluate the overall effectiveness of ERM
Assessing the Effectiveness of ERM

• Assess current state against 20 principles
  – Questions on each principle
  – Nature of evidence for each principle

• Identify gaps to desired level for each principle

• Determine actions to close gaps

• Refer to new Practice Guide for other guidance
Compendium of Examples

The compendium illustrates:

• All principles

• A variety of entity sizes from global through to national, regional, and local entities

• Actual company practices and augmented with expected practices in select areas, as needed

• An ERM perspective from the business mindset
---

**Principles Illustrated in Compendium**

- ♦ Primary examples
- * Secondary illustrations

<table>
<thead>
<tr>
<th>PRINCIPLE</th>
<th>Higher Education</th>
<th>Government</th>
<th>Financial Services</th>
<th>Energy</th>
<th>Not-for-Profit</th>
<th>Consumer Products</th>
<th>Technology</th>
<th>Industrial Products</th>
<th>Healthcare</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>♦ ♦ ♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>♦ ♦ ♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>♦ ♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>♦ ♦ ♦ ♦</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Top 5 Global Risks: likelihood

<table>
<thead>
<tr>
<th>2019</th>
<th>Asset price collapse</th>
<th>Slowing Chinese economy (&lt;6%)</th>
<th>Chronic disease</th>
<th>Global governance gaps</th>
<th>Retrenchment from globalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Top 5 Global Risks: impact

<table>
<thead>
<tr>
<th>2019</th>
<th>Asset price collapse</th>
<th>Retrenchment from globalization (developed)</th>
<th>Oil and gas price spike</th>
<th>Chronic disease</th>
<th>Fiscal crises</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2013</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2015</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2016</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2017</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2018</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Source: WEF 2019

The Global Landscape Continues to Shift

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

- Asset price collapse
- Slowing Chinese economy (<6%)
- Chronic disease
- Global governance gaps
- Retrenchment from globalization
- Oil and gas price spike
- Chronic disease
- Fiscal crises
- Extreme weather events
- Failure of climate-change mitigation and adaptation
- Natural disasters
- Data fraud or theft
- Cyberattacks
- Weapons of mass destruction
- Failure of climate-change mitigation and adaptation
- Extreme weather events
- Water crises
- Natural disasters
Companies have been Impacted by the Changing Business Context
Growing Interest from Investors in a Company’s ESG Performance

Almost half of 2018 shareholder proposals (US) were environmental and social related:

- Environmental and social shareholder proposals (2018)
- Link executive pay to environmental and social considerations
- Review or report on greenhouse gas emissions
- Report on sustainability
- Address human rights
- Political spending
- Lobbying activities

Institutional investors surveyed agreed that for too long, companies have failed to consider environmental and social risks and opportunities as core to their business.
Joint COSO/WBCSD Guidance on ESG Risks
Potential Updates to Existing Guidance

- Monitoring Guidance
- Understanding and Communicating Risk Appetite
- Practical Approaches to Creating and Protecting Organizational Value
- COSO in the Cyber Age
- ERM for Cloud Computing
Potential New Guidance

- Using COSO ERM to Manage Compliance Risks
- Blockchain and its Impact on Internal Controls and Risk
- ERM in an Agile Environment
- Psychology and Sociology of Fraud
- Assessment Tools for Risk
- Robotic Process Automation and Artificial Intelligence (no known authors at this time)
Summary

• COSO ERM focuses on:
  – Integrating with strategy and performance
  – Creating, preserving and realizing value
  – Enhances decision making

• Drives better internal auditing

• Can be applied across all industries and organizations of any size

• New guidance may be on its way to help