Auditing Enterprise Risk Management (ERM)

Bailey Jordan, Partner, Risk Advisory Services

April 11, 2017
Topics

- **Current State of ERM**
- COSO and ISO 31000 ERM Update
- ERM Maturity Models
- Auditing ERM Case Study
- Q&A
Current State of ERM

We still have some work to do…

- Most leaders believe the risks they face are complex and numerous
- Less than half describe risk management processes as "mature" or "robust"
- Most organizations are struggling to integrate risk management with strategic planning
- More organizations are establishing management-level risk committees
- Strong majority of boards are asking for increased senior executive involvement in risk oversight

Current State of ERM (Cont’d)
Common ERM Questions

- We manage risks every day. How is ERM different?
- We have committees assigned with specific risks. How are these efforts integrated with an ERM initiative?
- How should we structure our ERM team?
- Where are we on a typical ERM maturity curve? Where should we be based on our size, complexity, and industry?
- What is a typical ERM process?
- How is ERM monitored and reported? To whom? How frequently?
- How do we get started?
Current State of ERM (Cont’d)
Benefits of ERM

• Potentially reducing the number and impact of “surprises”
• Focuses management attention on the truly important risks
• Linking business decision making such that returns align with risks taken
• Increasing stakeholder confidence and value
• Enhancing transparency and accountability in overall organizational structure
Topics

- Current State of ERM
- **COSO and ISO 31000 ERM Update**
- ERM Maturity Models
- Auditing ERM Case Study
- Q&A
Common Risk Management Frameworks

There are several risk management frameworks. The most common are:

- COSO ERM
- ISO 31000
- Basel Accord
- King III
- Financial Stability Board (FRB)
- Other (internal)
COSO ERM vs. ISO 31000

COSO ERM and ISO 31000 have much more in common, than differences. Key differences are:

- ISO risks include events with positive and negative consequences
- COSO addresses inherent and residual risks; ISO focuses on residual
- ISO analyzes likelihood at the consequence level, not just the event level
- COSO focuses more on risk appetite, tolerance, risk culture and velocity

Source: Manoj Kulwal, CRO, RiskSpotlight, https://www.youtube.com/watch?v=3wh5rAUKQB8
Project to Update Enterprise Risk Management – Integrated Framework

• Announced in October 2014
• Update the 2004 *Enterprise Risk Management–Integrated Framework*
• Goal of:
  – Enhancing the framework’s content and relevance in an increasingly complex business environment
  – Enabling organizations worldwide to attain better value from their enterprise risk management practices
Why Update the ERM Framework Now?

• Since 2004, the market has continued to evolve and the COSO Framework is evolving with it
• The update will address the call for:
  – Elevating enterprise risk management concepts and practices as the bar continues to rise
  – Incorporating lessons learned from recent crises
  – Responding to business and operating environments that are more complex, technologically driven, and global in scale
  – Increasing stakeholder engagement and greater transparency and accountability
  – Increasing prominence of discussions at the board level
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 albeit 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
Why Change the Title of the Framework

- Retitles the framework as *Enterprise Risk Management*—Aligning Risk with Strategy and Performance
- Recognizes the importance of strategy and entity performance
- Delineates between internal control and enterprise risk management
- Integrates enterprise risk management with decision making
1. Updates Components and Adopts Principles
ISO 31000

ISO 3100, *Risk Management – Guidelines* is being updated:

- Public exposure draft open 2/17/17 to 5/11/17
- Consists of Principles, Framework and Process
  - Principles should enable an organization to manage the effects of uncertainty on its objectives
  - The Framework encompasses the organizational arrangements for designing, implementing, evaluating and improving the use of risk management
  - The Process provides a consistent structured approach to establishing context, risk assessment and risk treatment, along with ongoing monitoring, review, communication and consultation

*Source: Draft International Standard, ISO/DIS 31000*
Topics

- Current State of ERM
- COSO and ISO 31000 ERM Update
- ERM Maturity Models
- Auditing ERM Case Study
- Q&A
In the fall of 2014, the AICPA published Enterprise Risk Management, Guidance for Practical Implementation and Assessment. The guide contains:

- ERM Concepts and Components
- ERM Program Development
- ERM Program Maturity Monitoring and Evaluation
- Appendix – Example Program Maturity Self-Assessment
  - Across 8 COSO ERM components
  - From Ad hoc, Nascent, Defined, Systematic, Mature
In November 2016, the ERM Initiative Faculty at the NC State University Poole College of Management, published *ERM Process Evaluation: Identifying Opportunities for ERM Program Enhancement*:

- Designed to assist senior executives and their boards in better understanding the strength and relevance of their organization’s existing risk oversight processes
- This tool can be used to determine whether the organization is applying best practices in ERM, and if not, what steps could be taken to further enhance their ERM process
- Evaluates nine key components of value-add, robust ERM process
ERM Framework: Grant Thornton Maturity Levels

- **Level 1 (Reactive)**
  - Ad Hoc
  - Lack of Senior Management/Board emphasis on risk
  - No common risk language
  - Individual capabilities

- **Level 2 (Siloed)**
  - Emerging
  - Stove-pipe risk management
  - Some coverage of risk areas
  - Some Senior Management/Board support

- **Level 3 (Top Down & Integrated)**
  - Structured
  - ERM policy and common language used and understood
  - Risk leader identified
  - Dedicated ERM resources
  - Risks identified and assessed across the entire organization
  - Proactive Senior Management/Board support

- **Level 4 (Systemic & Strategic)**
  - Leveraged
  - Defined and disciplined process
  - Policy guidelines followed across the organization
  - Risk culture embedded into fabric of the organization
  - Consistent and frequent risk reporting to Senior Management and Board
  - Integrated with business processes

- **Level 5 (Optimized)**
  - Optimized
  - Link to strategic planning and budgets
  - Risk management used as a competitive advantage
  - Quantification of risk appetite and tolerance
  - Real-time analysis of risk portfolio and dash boarding
Topics

• Current State of ERM
• COSO and ISO 31000 ERM Update
• ERM Maturity Models
• Auditing ERM Case Study
• Q&A
IA conducted an internal audit of ABC’s Enterprise Risk Management (ERM) Program. The scope of the audit consisted of an independent review of ABC’s key ERM elements and process to provide the Audit Committee feedback on the effectiveness of the program.

Objectives

- Gain an understanding of the key processes related to the effectiveness of ABC’s ERM program, including risk identification processes and impact assessments
- Identify risks associated with these processes
- Assess adequacy of the monitoring and reporting to mitigate these risks
- Test the effectiveness of the program’s implementation
- Make recommendations for improvement
Audit Scope

• Program methodology including setting and aligning risk appetite to business activities
• Assess elements of the ERM program to criteria established by Standard and Poor’s
• Management’s involvement including accountability for risk management
• Effectiveness of risk identification and reporting of status
• Self-assessment of the group’s effectiveness by the Risk Steering Committee (RSC)

IA reviewed ABC’s ERM documentation and interviewed key personnel. IA documented observations in an Enterprise Risk Management Framework and findings in the Results section of this report. In addition, IA reviewed audit results during an exit meeting with key organization management.
Audit Approach

• Reviewed ERM documentation, e.g., charters, governance structure, risk self-assessment, action plans, Risk Steering Committee (RSC) minutes, Audit Committee reports, etc.

• Interviewed executives to gauge their working knowledge of ABC’s ERM program and to understand what is working well and what can be improved

• Benchmarked ABC’s ERM program against:
  – A framework developed jointly by the American Institute of Certified Public Accountants (AICPA) and Chartered Institute of Management Accountants (CIMA)
  – Industry peers
  – Leading practices in ERM, including Grant Thornton’s ERM Maturity Model
Audit Approach (cont’d)

• Benchmarked ABC’s ERM program against: (continued)
  – The Corporate Executive Board Company’s (CEB), ERM Maturity Diagnostic Attributes (14 attributes across Risk Governance, Risk Culture and ERM Life Cycle)
  – S&P’s *Methodology: Assessing Management’s Commitment to and Execution of Enterprise Risk Management Processes*
  – The Institute of Internal Auditors’ (IIA) position papers on the “3 lines of defense model” and “Internal Audit’s role in ERM”
Using the AICPA and CIMA Case Study, IA gauged the maturity of ABC’s ERM program. The remainder of this section presents the high level results of that evaluation.

<table>
<thead>
<tr>
<th>Category</th>
<th>Number of Criteria</th>
<th>Total Score Possible</th>
<th>Raw Score for Category</th>
<th>Percentage Score for Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Culture</td>
<td>12</td>
<td>60</td>
<td>60</td>
<td>100%</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>10</td>
<td>50</td>
<td>50</td>
<td>100%</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>13</td>
<td>65</td>
<td>61</td>
<td>94%</td>
</tr>
<tr>
<td>Articulation of Risk Appetite</td>
<td>5</td>
<td>25</td>
<td>17</td>
<td>68%</td>
</tr>
<tr>
<td>Risk Response</td>
<td>12</td>
<td>60</td>
<td>54</td>
<td>90%</td>
</tr>
<tr>
<td>Risk Reporting</td>
<td>6</td>
<td>30</td>
<td>23</td>
<td>77%</td>
</tr>
<tr>
<td>Integration with Strategic Planning</td>
<td>10</td>
<td>50</td>
<td>47</td>
<td>94%</td>
</tr>
<tr>
<td>Assessment of ERM Effectiveness</td>
<td>7</td>
<td>35</td>
<td>29</td>
<td>83%</td>
</tr>
<tr>
<td>Total Score</td>
<td></td>
<td>375</td>
<td>341</td>
<td></td>
</tr>
<tr>
<td>Grand Percentage</td>
<td></td>
<td>100%</td>
<td>91%</td>
<td></td>
</tr>
</tbody>
</table>
What’s Working:

• Overall Conclusion - ABC is a Very High 4 in the ERM Maturity Model (on a scale of 1 to 5 with 5 being the highest), with elements of level 5

• Risk Steering Committee – This committee effectively provides focus and support to Executive Management in fulfilling their duty to maintain an effective risk management and internal control environment

• Internal Audit – IA effectively evaluates the ERM processes and the management and reporting of key risks

• All levels of the organization interviewed (Audit Committee, EVP, SVP) have a good understanding of risk assessment process and tools and are directly involved in identifying, prioritizing, managing and monitoring risks
What Could be Improved:

- **Risk Appetite and Tolerance** – These should be formalized at the organization wide and/or business unit level to ensure alignment with the individual risk treatment strategies.

- **Audit Committee/Board Reporting** – Too much detail is being provided; need more summary information; need clearer communication of weighting/rating of the risks; and want more opinions and judgments from the Risk Steering Committee.

- **Risk Owner Accountability** – Risks are assigned Risk Owners. The Risk Steering Committee and Risk Management (2nd line of defense) and Internal Audit (3rd line of defense) monitor the Risk Owners’ responses and actions. More frequent and wide-spread reviews would ensure the Risk Owners are staying within the desired risk appetites and tolerances.
Audit procedures indicate that ABC’s ERM program is at a very high level of maturity. There is a well-defined process supported by tools, templates and reporting, demonstrating the organization’s commitment to risk management. Additionally, ABC’s ERM program has evolved over the past four-plus years:

– In the first two years, there was significant effort to educate and develop an initial risk universe, risk rankings and control objectives and activities. A bottoms-up approach was taken to build-out the risk universe
– In the subsequent years, ABC refined the approach, particularly the risk self-assessment process, and added a top-down risk approach
– All risks to the organization are considered (strategic, financial and operational), including opportunity risks
ERM is well coordinated with other compliance functions across the organization.
ERM documentation format is easy to use and well understood throughout the organization.
Management, the Audit Committee and Board receive regular reports on the risk environment and status of the most critical risks.
Today, the program appears to be at the appropriate level and balance with operations.
• ABC’s ERM maturity is at a very high 4, with elements of level 5
• The question is should ABC strive to, and consistently maintain a level 5 ERM maturity? Given the size, complexity and future plans, the costs may outweigh the benefits. Therefore, as appropriate, ABC should consider the following tweaks to the present ERM maturity:
  – More formally discuss opportunity and emerging risks
  – Consider velocity (speed of onset) during the risk assessment process
  – Review risk interrelationships
  – Further define risk appetite and tolerance for the highest risks
  – For the highest risks, enhance risk monitoring through KPI’s
Questions
Contact information

Bailey Jordan, Partner
Risk Advisory Services
T 919.881.2790
Bailey.Jordan@gt.com