Agenda

- Background on COSO ERM Framework
- How COSO Compares with Other Frameworks
- The Role of the IIA
- Questions
The COSO ERM Framework Project

- COSO initiated the developmental project in 2001
- Issued final framework in September of 2004
- Companies were predominately focused on financial reporting controls at the time
- A lot has happened since issuance
The Current State of ERM

For companies participating:

- **63%** see change in volume and complexity of risks over last five years
- **76%** communicate key risks on ad hoc basis
- Almost **70%** don’t routinely report the entity’s top risks to the board
- **48%** must improve KRI reporting to senior executives
- Risk management processes are relatively immature and ad hoc

S&P Has Reinforced the “Immaturity” Message

Current state at most nonfinancial companies across a wide variety of sectors*: 

- Less than a majority of companies have a "formal ERM program"
- Most "formal ERM programs" have generally just come under development
- The most common approach is to maintain a “risk register” or “heat map” that classifies the top risks by likelihood and severity along with a mitigation strategy for each
- Fewer companies assign specific ownership for key risks, develop alternative mitigation strategies and communicate risk tolerances clearly across their organizations
- Very few companies have a culture that integrates risk assessment into strategic decision-making, clearly communicates risk appetite and have a fully engaged board of directors overseeing risk

The Current State of ERM – A Summary

ERM is relatively immature

For many companies, ERM has either:

• Not been implemented
  
  or

• Has been implemented in a manner that adds limited value in strategy setting

Risk is often an afterthought to strategy and risk management is an appendage to performance management
Six Implementation Issues

(1) Rarely enterprise-wide or integrated with strategy-setting
(2) Too granular and mired into minutiae, losing interest of the C-Suite
(3) Sometimes gets implemented as an assurance initiative, not as a way to better run and manage the business
(4) COSO Framework designed as an evaluation tool, not as an implementation tool
(5) ERM is a journey
(6) Only in the last 18 months or so have many companies and their boards started to warm up to the notion of implementing some form of ERM
COSO ERM-Related Initiatives

Currently conducting a survey – the preliminary results:

- 461 respondents and U.S. centric
- 40.7% publicly traded, 35% private, for-profits
- 57.9% look to the COSO ERM framework
- 66.6% selected a score of 4 or 5 on a scale where 1 = "Not at All" and 5 = "A Great Deal" when responding to the statement that they believe the "COSO ERM Framework provides theoretically sound principles and guidance for ERM"
- Only 25% selected a 4 or 5 response (using the same scale) to the statement that "COSO ERM provides clear and practical direction and guidance for the implementation of ERM"

Turning to thought leadership:

- Recently issued two thought papers
- “Getting Started” coming out soon
- Three others in the pipeline: “Risk Appetite”, “Key Risk Indicators” and the results of a survey on the current and desired future states of the board risk oversight process
Discussion of Strengths and Weaknesses of COSO Framework
Comparison with COSO Framework
with Other Frameworks
Do We Need a Global Framework?

• Frameworks have a role

• There are other important factors, some of which are “conditions precedent” for risk management to function effectively

• We need a market-facing statement of the problem we are trying to solve
## Five Realities for Every CEO and Board

<table>
<thead>
<tr>
<th>Reality</th>
</tr>
</thead>
<tbody>
<tr>
<td>The time may come when the fundamentals of your business are about to change</td>
</tr>
<tr>
<td>It is not what you know that matters; it is what you don’t know that makes the difference between winning and losing</td>
</tr>
<tr>
<td>Your business is boundaryless and is not an island in and of itself</td>
</tr>
<tr>
<td>Sooner or later, there will be a crisis that will test your company</td>
</tr>
<tr>
<td>Management and directors are struggling with delineating between risk management and risk oversight</td>
</tr>
</tbody>
</table>

Are the available frameworks helping business leaders advance the dialogue?
The IIA’s Role

• Compare the various ERM frameworks and develop a point of view of the strong points of each

• Any determination that a “global framework” is needed or the IIA should “endorse” one framework over another should be based on a market-facing view

• What problem are we trying to solve?

• Risk management does not function in isolation

• Given that the IIA definition of internal auditing recommends a consultative approach, the question arises as to whether the internal auditing profession needs to up its game to remain relevant
Is Role of IA in Risk Management Adequately Defined and Is IIA Guidance Sufficient?

• The challenge lies more with skillsets and comfort level, including transitioning away from current perceptions and expectations of IA’s role

• The final frontier for the profession

• Demands skilled maneuvering by the CAE and a staff equipped with the skills to back up his or her commitments

• Won’t happen overnight

• Whether IIA can do more, a fact-based assessment of what the IIA is currently doing would be helpful
IIA Recommendations to COSO

• Regarding a global standard:
  – A major undertaking
  – Unclear what problem a global framework would solve that existing frameworks cannot address
  – Doubtful a new framework is going to solve the issues that compromise risk management
  – If ERM is not required by regulatory authorities on a global basis, what is the value proposition?

• Re IIA's Research Foundation:
  – Compare existing frameworks using appropriate criteria and identify strong points
  – Define market-facing issues pertaining to risk management
  – Using the market-facing issues as a context, develop a point of view regarding whether or not improvements are needed

• Three Options:
  – “Mine’s better than yours”
  – Throw away what we’ve got and start over with a global framework
  – “Use ‘em all” and drive continuous learning