Agenda

• General understanding of ERM
• Benefits of COSO ERM update
• Summary and Enhancements of Updated Framework
• Components of an ERM Framework
• Internal Audit’s Role in ERM
ERM OVERVIEW
**Why ERM?**

Business volatility, complexity and increasing risk is dominating the landscape for all organizations. Boards have started to respond but the journey is challenging and new thinking is needed if risk management is to improve resilience and enhance value creation.

<table>
<thead>
<tr>
<th>Business volatility and economic uncertainty are here to stay – increasing resilience is the order of the day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business model complexity is stifling performance and creating inefficiency</td>
</tr>
<tr>
<td>Speed of business change is rapid – increased speed of response and corporate agility is needed</td>
</tr>
<tr>
<td>The current internal and external environment has created increased risk, risk complexity and risk velocity</td>
</tr>
<tr>
<td>Exercising control across the business model is challenging - dominated by a critical web of third party relationships and geographic spread</td>
</tr>
<tr>
<td>The emergence of new/changed risks requires improved oversight rigor and access to new skill sets</td>
</tr>
</tbody>
</table>

“It is impossible, as an executive, to separate risk from broader business issues – and in many cases the most important variable – in every decision made in business” *Ian Tyler, CEO, Balfour Beatty Plc – March 2011*

**Stakeholders** are asking more demanding answers to more challenging questions - *regulation* continues to drive onerous compliance requirements.
Benefits of ERM

- Increase the range of opportunities – By considering all reasonable possibilities, management can identify opportunities for the entity and unique challenges associated with current opportunities.
- Identify and manage entity-wide risks – Every entity faces myriad risks that can affect many parts of the entity.
- Reduce surprises and losses – ERM allows organizations to improve their ability to identify potential risks and establish appropriate responses, reducing surprises and related costs or losses.
- Reduce performance variability – For some entities, the challenge is less about surprises and losses, and more about performance variability.
- Improve resource deployment – Obtaining robust information on risk allows management to assess overall resource needs and enhance resource allocation.
Traditional Risk Management vs. ERM

**Traditional Risk Management**
- Tactical, compliance focused
- Silo-based processes
- Business line or risk type view
- Looks at risks individually
- Business decisions not closely linked to risks
- Driven by Risk Management and Internal Audit
- Supported by rules

**ERM**
- Strategic, performance focused
- Consistent risk management approach across the enterprise
- Holistic view of key risks
- Considers risk interactions
- Business decisions based on a clear understanding of risks
- Driven by the board and owned by the business
- Supported by a “risk culture”
Enhancements To the Updated Framework

• Provides greater insight into the role of enterprise risk management when setting and executing strategy.

• Enhances alignment between performance and enterprise risk management.

• Accommodates expectations for governance and oversight.

• Recognizes the globalization of markets and operations and the need to apply a common, albeit tailored, approach across geographies.

• Expands reporting to address expectations for greater stakeholder transparency.

• Accommodates evolving technologies and the growth of data analytics in supporting decision-making.
COSO ERM Framework

Mission, Vision, and Core Values

1. Exercises 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

Strategy and Business Objectives

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
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
18. Uses Relevant Information
19. Leverages Information Systems
20. Communicates Risk Information
21. Reports on Risk, Culture, and Performance
22. Monitors Substantial Change
23. Monitors Enterprise Risk Management Performance

Enhanced Performance
5 Components of COSO ERM Framework

1. Risk Governance and Culture
2. Risk, Strategy, and Objective Setting
3. Risk in Execution
4. Risk Information, Communication and Reporting
5. Monitoring Enterprise Risk Management Performance
Risk Governance

- Reviews and approves risk strategies, frameworks, and policies
- Reviews risk reports and recommends/monitors risk limits and action plans
- Oversees the implementation of the ERM framework/controls

ERM / Risk Officer

ERM function
- Risk policies
- Incentives
- Product/strategy review
- Risk appetite
- ERM training

Board oversight
Risk Culture

Development of a risk culture is critical to effective ERM

Ways to establish a risk culture that is supportive of risk management:

• “Tone at the top”
  – Reference the importance of risk management in organization’s objectives
  – Incorporate risk management into ongoing executive management communications
  – Exhibit the desired risk management behaviors

• Code of Conduct or Ethics

• Risk management factors included in incentive and performance evaluation plans

• Clearly defined roles and responsibilities that are consistent with three lines of defense
Risk Appetite

• An effective ERM program relies on the establishment and communication of the organization’s risk appetite
  – Helps employees to understand the specific risks that the organization is willing and not willing to take.
  – Provides a means for ensuring that actual risk-taking is consistent with the organization’s risk-taking capacity.

• There are many ways to define risk appetite:
  – Statements, such as “a zero tolerance for compliance risk” or “target debt rating of AAA”
  – Specific products, markets and/or customer segments that are outside of the company’s risk tolerance
  – Metrics that define risk thresholds, such as financial measures (e.g., ROE target) or limits (e.g., % of total risk exposure)
Risk Appetite Expressions

• Example 7.4: Sample Risk Appetite Expressions

• **Target:** A credit union with a lower risk appetite for loan losses cascades this message into the business by setting a loan loss target of 0.25% of the overall loan portfolio.

• **Range:** A medical supply company operates within a low overall risk range. Its lowest risk appetite relates to safety and compliance objectives, including employee health and safety, with a marginally higher risk appetite for its strategic, reporting, and operations objectives. This means reducing to a reasonably practicable amount the risks originating from various medical systems, products, equipment, and the work environment, and meeting legal obligations will take priority over other business objectives.

• **Ceiling:** A university accepts a moderate risk appetite as it seeks to expand the scope of its offerings where financially prudent and will explore opportunities to attract new students. The university will favor new programs where it has or can readily attain the requisite capabilities to deliver them. However, the university will not accept programs that present severe risk to the university mission and vision, forming a ceiling on acceptable decisions.

• **Floor:** A technology company has aggressive goals for growth in its sector, and recognizes that such growth requires significant capital investment. While it does not accept investing capital unwisely, management is of the view that, as a minimum, 25% (i.e., the floor) of the operating budget should be allocated to the pursuit of technology innovation.
Example 7.6: Cascading Risk Appetite

**Mission:** To provide healthy, great-tasting premium organic foods made from locally sourced ingredients.

**Vision:** To be the largest producer of sustainable sourced organic products in the markets we serve.

**Core Values:** We work to achieve a healthy environment that is sustainable. We will use ingredients grown only in natural composts, non-altered crops, and soil rich in organic life.

**Strategy:** To build brand loyalty by producing food that is delicious and exciting, that people want to eat because it tastes good, not because it is good for them.

**Risk Appetite:** Brand is essential to us. We will strive to be innovative to develop products that meet customers' preferences. We will not put cost above our core values, product quality, or ingredient choice. Nor will we put growth above sustainable operations.

**Business Objective:** To continue to develop new, innovative products that interest and excite consumers.

**Risk Appetite:** We will continue to strive to be innovative and find new tastes.

**Risk Appetite:** We will not compromise our brand by using products that are not certified organic. We accept that this may increase our cost.

**Business Objective:** To expand our retail presence in the higher-end health food sector.

**Risk Appetite:** We value our brand as a premium product and will focus only on those retailers that share our core values. We understand that this may affect our sales channel.
Risk Management Processes

• Risk management processes are grouped in different ways but generally include the following:

• Ideally, each of these processes should be ongoing rather than, for example, annual.
Risk Identification

• Risk identification processes should begin with appropriate planning:
  – Mapping of the company’s business lines and processes
  – Determination of the risk types to be included in the process (e.g., operational, legal, reputational)
  – Identification of resources responsible for the process in each area

• Risks can be identified through various methods, such as interviews, surveys and/or facilitated workshops
  – Different levels of the organization may have different perspectives on risks
  – Include emerging risks
  – Be wary of risks that are really the absence of controls
Risk Assessment

• Risk assessment should begin with clarification of the objectives
  – Business line and Internal Audit risk assessments have different purposes (e.g., prioritization of risks vs. basis for audit plans)
• Common definitions, including inherent vs. residual risk, risk levels, and the adequacy of controls, should be clearly communicated.

For example:
  – A risk with a “high” likelihood may result in losses on a daily basis;
  – A risk with a “high” impact may result in a loss equal to X, or significant harm to the organization’s reputation.
Risk Assessment

• Best practices in risk assessment include:
  – Identification of risks against key business objectives
  – Coordination of risk assessments through interviews, surveys or facilitated workshops to ensure consistency
  – Use of available information, such as Key Risk Indicators (KRIIs), to ensure objectivity

• Assessments of the adequacy of internal controls must also be objective
  – Oversight and use of information, such as the results of quality control reviews, are critical
Risk Heat Map - Example

Extraordinary events – often overlooked

Secondary risks - focus on controls

Lower priority – focus on efficiency

Strategic imperatives

Likelihood

Impact

High

Low

High
Risk Response

• Risk responses should be based on assessment of loss frequency and impact
  – Management actions should be specific to reducing likelihood or impact, depending on which one was assessed as high

The most common risk responses include:
  – **Avoid** (get out)
  – **Accept/retain** (monitor)
  – **Reduce** (institute controls)
  – **Transfer or share** (partner with someone)

• Action plans with assigned owners should be developed and monitored
Risk Monitoring

• Risk monitoring should follow from risk assessments
  – Higher risks should be monitored more frequently and in more depth

• Key risk indicators (KRI) are critical to early identification of risks and, as a result, fewer surprises
  – KRI should be forward-looking
  – Key Performance Indicators (KPI) are primarily backward-looking
Risk Reporting

• Reporting should also follow from risk assessments, with higher risks reported in more depth

• Emphasis of risk reporting should be on highlighting key risks and recommendations for and status of management action

• Volumes of detail should be avoided, particularly for board reporting

• Reports should include early indicators and emerging risks

• Best practices include the development of ERM dashboards that provide a holistic view of risk and thoughtful analysis
Integrating ERM into decision-making

- To be effective, risk management must be integrated into day-to-day business line activities and corporate decisions
  - Risk assessment must be done as part of the strategy setting processes
  - Risks associated with new products / projects / programs should be considered and communicated to the board
  - Analysis of emerging risks should influence business decisions
  - Risk information should be shared across the organization to avoid the same event recurring
Lessons Learned

• Tone at the Top
• Crawl-Walk-Run
• Build on Tools / Processes in Place
• Simplicity at the Outset
• Culture – Culture – Culture
INTERNAL AUDIT’S ROLE IN ERM
ERM today

• Many companies are at early stages of implementing an effective organization wide approach to managing risk
• Implemented ERM programs have had mixed results
  • From poorly defined programs without depth - overly comprehensive and bureaucratic programs that offer little value
• Opportunities for Internal Audit to review the effectiveness of existing ERM programs and/or play an advisory role in its development or enhancement
State of ERM…

• 25% believe their organization has a “complete formal enterprise-risk management process in place”

• 23% describe their organization’s level of risk management maturity as “Mature” or “Robust.”

• 52% indicate that their organization’s risk management process is “not at all” or “minimally” viewed as a proprietary strategic tool that provides unique competitive advantage.

Source: 2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities - Research Conducted by the ERM Initiative at North Carolina State University on behalf of the American Institute of CPAs Business, Industry & Government Team
Calls for Improved Enterprise-Wide Risk Oversight…

• 68% indicate that the board of directors are asking for more senior executive involvement in risk oversight.

• 65% of organizations experience more pressure from external parties to provide more information about risks.

Source: 2015 Report on the Current State of Enterprise Risk Oversight: Update on Trends and Opportunities - Research Conducted by the ERM Initiative at North Carolina State University on behalf of the American Institute of CPAs Business, Industry & Government Team
Who’s responsible for ERM at your organization?

• Over past 15 years, organizations have tapped Internal Audit functions to help establish ERM processes.

• IA has ingredients to effectively push ERM:
  – Knowledge of the organization across all areas (not just financial)
  – Experts at risk and control evaluations
  – Relationships at the C-Suite and Board / Audit Committee levels

• But…independence may be compromised depending on the ongoing role IA plays
Internal Auditing’s role in ERM

Source: IIA–Assessing the Adequacy of Risk Management, December 2010
Core function – Assurance on risk management

- Evaluation of an organization’s ERM program with a focus on:
  - Framework used / completeness (e.g. COSO, ISO 31000, etc.)
  - Methodology
  - Executive sponsorship
  - Board support
  - ERM charter and process framework
  - Risk policies
Review management of key risks

- Risk management based auditing ensures there is an understanding and alignment with business objectives and not just business risks. It evaluates the maturity of the risk management activity and gives consideration to management’s risk appetite in reporting.

<table>
<thead>
<tr>
<th>Three activities Internal Audit can perform with risk management auditing</th>
<th>Targeting risks as opposed to processes in auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitoring risk management maturity</td>
</tr>
<tr>
<td></td>
<td>Communicating detailed audit reports organized by risk rather than process</td>
</tr>
</tbody>
</table>

©2017 RSM US LLP. All Rights Reserved.
Looking for Risk in All the Wrong Places
Risk management has historically focused more than half its time on legal, compliance, and financial-reporting functions. That’s starting to change as companies realize that most big hits to shareholder value come from strategic and operating risks.

THE PROPORTION OF SIGNIFICANT LOSSES IN MARKET VALUE CAUSED BY EACH TYPE OF RISK OVER THE PAST DECADE

<table>
<thead>
<tr>
<th>Type</th>
<th>Proportion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>86%</td>
</tr>
<tr>
<td>Operating</td>
<td>9%</td>
</tr>
<tr>
<td>Legal and compliance</td>
<td>3%</td>
</tr>
<tr>
<td>Financial reporting</td>
<td>2%</td>
</tr>
</tbody>
</table>

THE PROPORTION OF TIME AUDITORS SPENT ON EACH TYPE

<table>
<thead>
<tr>
<th>Type</th>
<th>Time Spent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>6%</td>
</tr>
<tr>
<td>Operating</td>
<td>13%</td>
</tr>
<tr>
<td>Legal and compliance</td>
<td>39%</td>
</tr>
<tr>
<td>Financial reporting</td>
<td>42%</td>
</tr>
</tbody>
</table>

SOURCE: CEB
FROM “HOW TO LIVE WITH RISKS,” JULY-AUGUST 2015

© HBR.ORG
Other activities

- Results of ongoing enterprise risk assessment considered in IA’s risk assessment and audit plan
- Assessment of responsibilities and effectiveness of lines of defense (1st and 2nd); coordination of testing where applicable
- Evaluation of risk reporting and senior executive and Board reporting
# Measuring Risk - Example

<table>
<thead>
<tr>
<th>Auditable entities</th>
<th>Degree of change</th>
<th>Growth of area</th>
<th>Complexity</th>
<th>Materiality</th>
<th>Susceptible to fraud</th>
<th>Previous results</th>
<th>Strategic Objectives</th>
<th>Enterprise Risks (Top 10)</th>
<th>ERM Score</th>
<th>Total Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>BU A - Pricing</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>3.4</td>
</tr>
<tr>
<td>Research and development</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3.3</td>
</tr>
</tbody>
</table>
Considerations for Internal Audit scope

In practice, organizations are still struggling to deliver a return on investment beyond compliance – the need to improve has never been greater.

| Execution remains the key challenge in practice | For many, the basics are not in place | The right risks are not on the table | Business / risk complexity has led to process complexity |
| Change is happening faster than our capacity to manage | Risk functions often don’t have the right remit | Risk appetite / tolerance has not been established |
| Focus still too much on Financial Risk, not on Operational and Strategic | Legacy process and structure is difficult to undo | Emerging process imperatives are in the ‘too hard tray’ for many |
| Managing the flow of information to the Board is a critical challenge to resolve | Program risk management lacks rigor and discipline | Key identified risks are not analyzed for appropriate mitigation |
Considerations in implementing ERM programs

Step 1: Getting the cultural fit right

- Understand the politics and culture of the organization
- Determine the key drivers as to why the company is implementing ERM
- Evaluate CEO / senior management support
- Solicit Board / Audit Committee input
- Link ERM to the strategic planning process
- Identify a risk champion and committee within the organization
- Possess the requisite industry expertise
- Develop consistent “risk language” and processes that make sense to the organization

*All of the above may not be achieved in year one*
Considerations in implementing ERM programs

Step 2: Considering the “three lines of defense” in the model

Risk Governance

Board

- Approves significant risk management policies
- Sets the tone-at-the-top in terms of ERM’s importance

Risk / Audit Committee

- Oversees the ERM program and alignment with strategy
- Reviews aggregate risk exposures and emerging risks
- Oversees financial reporting and internal controls

Management Risk Committee

- Implements ERM into culture
- Reviews and discusses new risks
- Reviews and recommends risk responses

Risk Management Processes

Risk identification, assessment, response, monitoring, reporting

Validation

Internal Audit

3rd Line of defense

- Audits compliance with risk management policies and procedures
- Audits the adequacy of internal controls
- Audits the ERM program
- Audits financials

Business functions

1st Line of defense

Risk Champions

2nd Line of defense
Considerations in implementing ERM programs

Step 3: Making ERM “stick” within the organization

- Influence the alignment of ERM and Internal Audit (i.e. on “auditable” risks)
- Prioritize ‘quick-wins’ by which ERM can enhance organizational communication on an important matter, decision support on a key topic, etc.
- Keep ERM activities aligned with strategic imperatives and “rewarded” risk-taking (i.e. keep the program close to the C-suite), as well as more traditional compliance/“unrewarded” risks
- ERM should provide value not previously realized within the organization (e.g. forums for communication, risk analytics, exposure to senior leadership by managers)
- Team with HR leadership to create/enhance innovative leadership development programs supporting risk management
- Continuously integrate industry insights / competitive intelligence into the process
This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.

RSM® and the RSM logo are registered trademarks of RSM International Association. The power of being understood® is a registered trademark of RSM US LLP.

© 2017 RSM US LLP. All Rights Reserved.