Agenda

1. Introducing COSO
   - Who is COSO and what is the COSO ERM Framework?

2. Why update the Framework now?
   - What prompted the Framework update?
   - What was the feedback received during Public comment?

3. What has changed?
   - How does this compare to the 2004 COSO ERM Framework and why were changes introduced?

4. What does it mean for you?
   - What does the new Framework mean for you and your organisation?

5. More information
   - How to obtain a copy of the new Framework and obtain more information

---

*COSO recognises the growing expectation of organisations to manage, in an integrated and cohesive manner, risks emanating from across an enterprise.*

Robert B. Hirth Jr., COSO Chair
Introducing COSO
COSO’s 2004 Enterprise Risk Management–Integrated Framework is one of the world’s most widely used risk management frameworks.

www.coso.org

COSO and PwC have collaborated on frameworks and publications for 25 years

Other COSO publications authored by PwC

- 2013 Internal Control – Integrated Framework Executive Summary
- 2013 Internal Control – Integrated Framework
- 2012 Understanding and Communicating Risk Appetite
- 2006 Internal Control over Financial Reporting Guidance for Smaller Public Companies
- 1992 Internal Control – Integrated Framework
What prompted the Framework update?
CEO confidence is rising....

Leaders are looking to ERM to give them greater confidence in managing the risks to the achievement of their strategy and business objectives

Question 1: Do you believe global economic growth will improve, stay the same, or decline over the next 12 months?

Question 2: How confident are you about your company’s prospects for revenue growth over the next 12 months and next 3 years?

Source: 2017 PwC 20th Annual CEO Survey
At the same time, many Boards are not receiving the information they need

Question: How often does your board get updates and reports from management on:

- The company’s key risks
- The amount of risk the company is taking (i.e., risk appetite)
- Changes to the company’s approach to enterprise risk management

58% of Boards do not receive updates at every meeting on the amount of risk the company is taking

Boards recognize that there are opportunities for ERM to add greater value

Question: How well do you believe management performs the following activities:

- Provides effective summary-level metrics and reporting to the board: 67% (Very), 32% (Somewhat), 1% (Not at all)
- Links risks to strategic objectives: 57% (Very), 41% (Somewhat), 2% (Not at all)
- Leads effective ERM efforts: 57% (Very), 43% (Somewhat), 1% (Not at all)
- Identifies longer-term risks related to economic, technological, geopolitical, and environmental trends: 44% (Very), 50% (Somewhat), 6% (Not at all)
- Reviews its crisis response plan: 55% (Very), 31% (Somewhat), 14% (Not at all)

So what are risk and business professionals saying?

I want an ERM Framework that drives improvements to business functions beyond risk avoidance.

As an innovative company, I want to use risk to create value and not only to protect value.

I want to reduce performance variability and respond more quickly to opportunities.

I need insights that help me understand risks and opportunities and evaluate strategic options.

When I develop my strategy, I want to have a full picture of the potential risks and the capabilities I need to create advantage.
Why update the ERM framework now?

- **Boards are expecting more** from their organisation’s ERM practices and capabilities
- Stakeholders are seeking **greater transparency** and accountability
- Business environments are increasingly **complex**, technologically driven, and global
- There is a need to **incorporate lessons learned** from recent events and the bar is rising
- Risk professionals are looking for a **more up to date resource** describing ERM concepts
- The range of ERM **practices continues to evolve**

Since 2004, the market has continued to evolve and the COSO Framework is evolving with it.
What’s changed?
A new framework with global input

As part of the drafting process, the Framework was made publicly available for review and comment between June and September 2016.
Key highlights from feedback received

Feedback received was reviewed by the project team and informed the final updates to the Framework prior to publication.

- **Letters and Surveys**
  - 217 online surveys submitted
  - 47 comment letters received
  - Relatively consistent volume of feedback compared to other COSO Framework projects

- **Comments**
  - 2,000 individual comments
  - Comments covered every section of the draft Framework
  - All comments reviewed by the PwC Project Team and categorised according to nature (e.g., conceptual, editorial, commentary etc.)

- **Themes**
  - Encouraging breadth of themes addressed in comments
  - Comments ranged from the highlighting conceptual differences, requests for clarity and suggested editorial changes

- **Feedback**
  - Positive ratings outnumbered negative by 4.5:1
**Introducing the 10 key changes to the 2017 Framework**

- **A new framework structure**—five components and twenty principles that align to the business lifecycle, making risk conversation more intuitive for you.
- **A focus on integrating risk management**—linking risk with strategy setting and day-to-day activities, helping you to use ERM principles to support the creation, realisation, and preservation of value.
- **Written from the perspective of the business**—risk management concepts are discussed in terms of helping an organisation create value, enabling you to realise true benefits from ERM.
- **Explores management of risk at all altitudes of the organisation**—from entity level through to procedural level risks, making ERM more than just an isolated view of risk in the business.
- **Greater emphasis on culture**—reflecting the changing demands and expectations of today’s markets, helping your organisation make responsible risk decisions.
- **Explores the different benefits of ERM**—from loss mitigation through to strategic advisor and how they inform the design of a risk framework.
- **Suites of new graphics highlighting the relationship between risk and performance**—demonstrating a new way to identify and assess the relationship between the amount of risk and the level of performance.
- **Deeper discussions on challenging topics**—such as risk appetite and the portfolio view of risk.
- **Addresses the evolving role of technology**—in influencing an organisation’s strategy, business context and how it manages risk.
- **Coming soon: Compendium of Examples**—highlighting the implementation of principles across a variety of industries and entity types.
A new **framework structure**

The graphic symbolizes the dynamic, integrated nature of ERM that begins with the mission, vision and core values of the organisation through to the creation of enhanced value.
The new Framework adopts a components and principles structure
Explores the benefits of ERM

**Increasing the range of opportunities**

- By considering all possibilities - both positive and negative aspects of risk - management can identify new opportunities and associated challenges.

**Identify and manage risks entity-wide**

- Management identifies and manages these entity-wide risks to sustain and improve performance.

**Increasing positive outcomes**

- Improve management’s ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses.

**Reducing performance variability**

- Management can anticipate the risks that would affect performance and put in place the actions needed to reduce disruption and improve opportunity.

**Improving resource deployment**

- Risk information enables management, in the face of finite resources, to prioritise resource deployment and enhance resource allocation.

**Enhancing enterprise resilience**

- Enhance management’s ability to anticipate and respond to change, not only to survive but also to evolve and thrive.

- Enterprise risk management frameworks are as varied as the organisations they support.
- In their infancy, many frameworks focus on increasing positive outcomes and identifying entity-wide risks.
- Boards, senior management and stakeholders are increasingly expecting ERM to reduce performance variability, improve resource deployment and enhance enterprise resilience.
- This will often require that the capabilities and practices of an organisation to evolve in line with increasing expectations.

- The effectiveness of an enterprise risk management Framework is founded on fostering, designing and implementing the culture, capabilities and practices that align to intended benefits.
- A more detailed discussion of the benefits of ERM can be found in the COSO Executive Summary.
**Focusing on integrating risk and strategy**

The strategy setting process is a critical area of integration for enterprise risk management

- Strategic blunders account for a majority of the losses in shareholder value compared to operational events, incidents or compliance failures

- Research suggests that organisations are looking to strengthen the integration between strategy and enterprise risk management

81% of the greatest losses in shareholder value since 2002 were attributable to ‘strategic blunders’

*U.S. public companies around the world with at least US$1 billion in enterprise value on January 1, 2002 (1,053 companies met these criteria), Dann, Le Merle and Pencavel, “The Lesson in Lost Value” Strategy+Business, November, 2012*
Focusing on integrating risk and strategy

The updated Framework elevates the discussion of integrating strategy and risk through three different dimensions:

1. The possibility of strategy not aligning with mission, vision and core values;
2. The implications from the strategy chosen; and
3. Risk to strategy and performance.
Explores managing risk at all altitudes of the organisation

The Framework highlights that **risks emanate and must be managed at all levels of the organisation**. The Framework explores how risks can manifest at multiple levels within an organization with some risks directly impacting the entity strategy while others impacting business objectives.

The Framework also addresses how **risks can change in severity and prioritization at different levels of the organisation** and how the impacts of correlation and diversification are considered when analysing the risk profile of portfolio view of risk.

- Risk frameworks should ensure existing risk identification and assessment practices account for risks occurring at different levels of the organisation
- Risk capabilities should account for how risk ratings and responses may exist and change at different altitudes within an organisation
- Management should designate appropriate roles and responsibilities for the management of risk and execution of risk responses
How the Framework emphasises technology

The Framework recognizes the importance of enterprise risk management keeping pace with technological developments

- The Framework emphasises how enterprise risk management practices and capabilities need to align with the velocity of changes to the business context, emerging and changing risks.

- Information, Communication and Reporting principles now have a greater focus on integrated risk and performance reporting.

- Developments in data generation and analytics including ‘big data’, artificial intelligence and social media have been acknowledged.

- Discussions on the accuracy, completeness and timeliness of data have been retained in the COSO Internal Control Integrated Framework.

Source: PwC Mega Trends – Technological Breakthroughs
The Framework was written from the perspective of the business to facilitate the integration of ERM and support acceptance and adoption by the business

- There is often a ‘siloed’ approach to risk that is separate from the day to day management of an organisation.
- Risk management is perceived as an incremental activity performed by those independent of the business.
- The lack of integration can contribute to difficulties engaging with the business, the ability to gain and offer insight and ultimately curbs the value that ERM can offer.

- The Framework endeavors to remove risk ‘jargon’ and adopts the language of business to discuss concepts and practices
- By using the same language, the Framework hopes to promote acceptance and adoption of ERM by the organisation

Note: In practice, ERM often refers to a team, department or as a part of the ‘lines of defense’ however, in the Framework it is discussed in the context of an organisation’s culture, capabilities and practices used to manage risk.
How the Framework addresses culture

Culture now features in the definition of ERM and is part of the Framework’s Governance and Culture Component

Principles on culture are now more focused on decision-making and the alignment to expected behaviors in line with the core values of the organization

The importance of aligning the core values and risk appetite of the organization to promote consistent and risk-based decision making

COSO ERM Definition
The culture, capabilities and practices, integrated with strategy setting and its execution, that organisation rely on to manage risk in creating, preserving and realising value

Discussions on the importance and commitment to integrity and ethics have been retained in the COSO Internal Control Integrated Framework
Deeper discussions on other challenging topics

Enhanced discussions on:
- Alignment of Risk Appetite and Strategy
- Delineation between risk appetite and tolerance
- Consideration of risk appetite as an evaluative vs decision-making tool
- Alignment of risk appetite to risk assessment and the portfolio view of risk

Additional focus on:
- Articulating risks relative to business objectives and performance
- Developing severity measures and prioritization criteria given the risk appetite of the organization
- Risk assessments at different levels including new illustrative graphics relating to aggregation

Greater detail provided on:
- Graphical representations of portfolio view
- Emphasis on an business objective centric view of risk
- Alignment to strategy and resource deployment
- Tie to integrated performance monitoring and reporting

Requests for additional guidance represented some of the most common feedback the PwC Project Team received during the Public Comment Period.
A compendium of examples is also being developed. The proposed compendium will illustrate:

- All principles;
- A variety of entity sizes from global through to national, regional, and local entities;
- A variety of industry types;
- Actual company practices and be augmented with expected practices in select areas, as needed; and
- Written from the perspective of the business.

Examples:

- Governance in a higher education institution
- Culture in a government entity
- Culture in a financial services company
- Strategy and objective-setting in an energy company
- Strategy and objective-setting in a not-for-profit entity
- Performance in a consumer products company
- Performance in a technology company
- Review and revision in an industrial products company
- Risk information in a healthcare company
What does this mean for you and your organisation?
What does this mean for Internal Audit?

**Assurance role:**
- Joint internal audit and ERM risk assessments to provide integrated view of risks
- Validating management’s action plans and assessing progress against those plans
- Auditing processes and controls that address higher risk areas
- Assessing maturity and effectiveness of ERM processes

**Consulting role:**
- Participate in strategy discussions to provide a point of view on risk implications of selected strategies
- Reviewing risk appetite framework of the organization
- Understanding how organization creates, realizes and preserves value and the supporting assumptions
- Encouraging risk professionals to sync with the language of business in the organization
- Spreading awareness within organization and challenging the organization to think about ERM as a process and not a function, department or standalone tool
How can Internal Audit help their organization get started.....

1) **Identify the benefits being sought** from ERM by your organization

2) **Determine the desired integration** of enterprise risk management within the organisation

3) **Prioritize the initiatives and resources** required to implement or enhance existing cultures, capabilities and practices

---

**Aligning Culture**

- Secure board and senior management endorsement for implementing or enhancing the Enterprise Risk Management Framework
- Incorporate risk management expectations into training and incentives to enhance consistency in decision-making
- Communicate and clarify roles and responsibilities for risk management

**Augmenting Capabilities**

- Invest in tools, templates or technology that support risk management activities and decision-making
- Include third party providers and vendors in discussions on risk and performance
- Encourage discussion of entity’s risk appetite and profile within governance forums and as part of management decision-making

**Enhancing Practices**

- Evaluate whether current practices align with desired integration and achieve benefits sought from ERM
- Review risk identification, assessment, prioritization and response processes for opportunities for enhancement
- Analyse reporting practices for opportunities to further integrate with performance

---

Percentage of respondents that stated implementation of effective ERM Frameworks as the most common challenge in deriving its expected benefits.
## How Boards can take a fresh look at risk oversight

<table>
<thead>
<tr>
<th>Key Challenges</th>
<th>Board Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>How can boards reassure investors that it is overseeing risks appropriately?</td>
<td>Enhance proxy disclosures to better describe risk oversight, so shareholders can better understand what your board does and how.</td>
</tr>
<tr>
<td>Are any key risks falling through the cracks?</td>
<td>Clearly allocate risk oversight among the board and its committees. Ensure that the chairs share their committees’ insights about those risks with the full board.</td>
</tr>
<tr>
<td>How can directors know if ERM is adding value?</td>
<td>Dig into how well ERM works and whether changes should be made.</td>
</tr>
<tr>
<td>How can the board ensure that executives take their responsibility for risk seriously?</td>
<td>Discuss with senior management how they have put ERM into practice, including who’s accountable for key risks and how ERM works at lower levels in the company.</td>
</tr>
<tr>
<td>How can the board better understand what risks may emerge in the future?</td>
<td>Push executives for regular forward-looking, strategic input on emerging risks.</td>
</tr>
<tr>
<td>How can the board get the reporting it really needs on risk?</td>
<td>Be clear on the kind of risk information you need from management and how often you want to see it.</td>
</tr>
</tbody>
</table>

Source: PwC Governance Insights Center – Risk Series
More information
Staying involved

Access the Framework at www.coso.org

View videos, blogs and articles at www.pwc.com/coso-erm

Amanda Herron  
Partner, Risk Assurance  
Tel: 704-724-5708  
amanda.c.herron@pwc.com

Meghana Dholabhai  
Director, Risk Assurance  
Tel: 214-608-1152  
dholabhai.meghana@pwc.com
Thank you