www.pwc.com

COSO Enterprise Risk Management Framework- Integrating Strategy and Performance

October, 2017

pwc

Agenda

1	2	3	4	5
Introducing COSO	**Why update the Framework now?**	**What has changed?**	**What does it mean for you?**	**More information**
Who is COSO and what is the COSO ERM Framework?	What prompted the Framework update? What was the feedback received during Public comment?	How does this compare to the 2004 COSO ERM Framework and why where changes introduced?	What does the new Framework mean for you and your organization?	How to obtain a copy of the new Framework and obtain more information

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

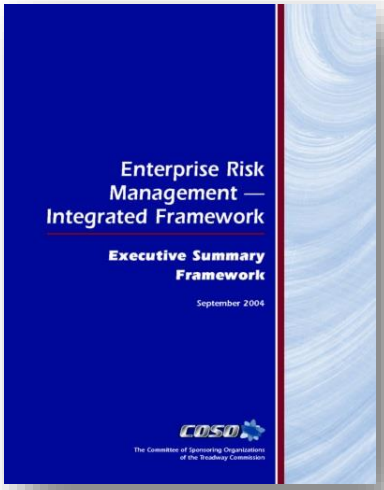
Robert B. Hirth Jr., COSO Chair

Introducing COSO

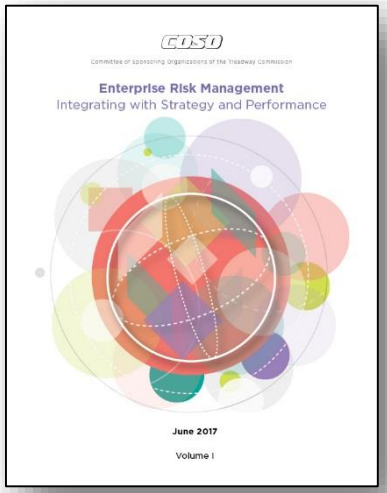
COSO's 2004 *Enterprise Risk Management-Integrated Framework* is one of the world's most widely used risk management frameworks.

www.coso.org

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

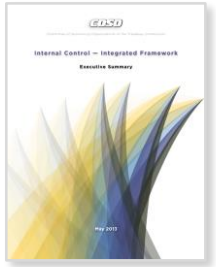


2004



2017 Publication

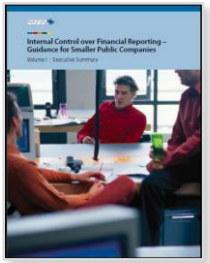
Other COSO publications authored by PwC



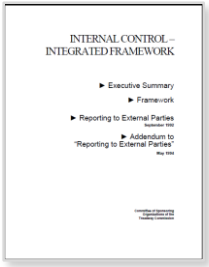
2013 Internal Control – Integrated Framework Executive Summary

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

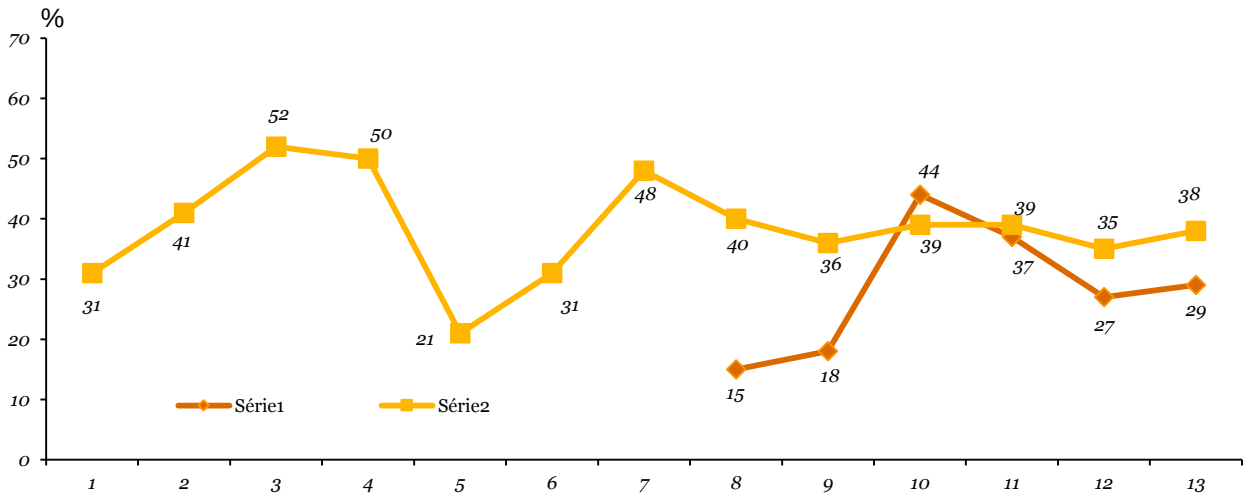
What prompted the Framework update?

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?

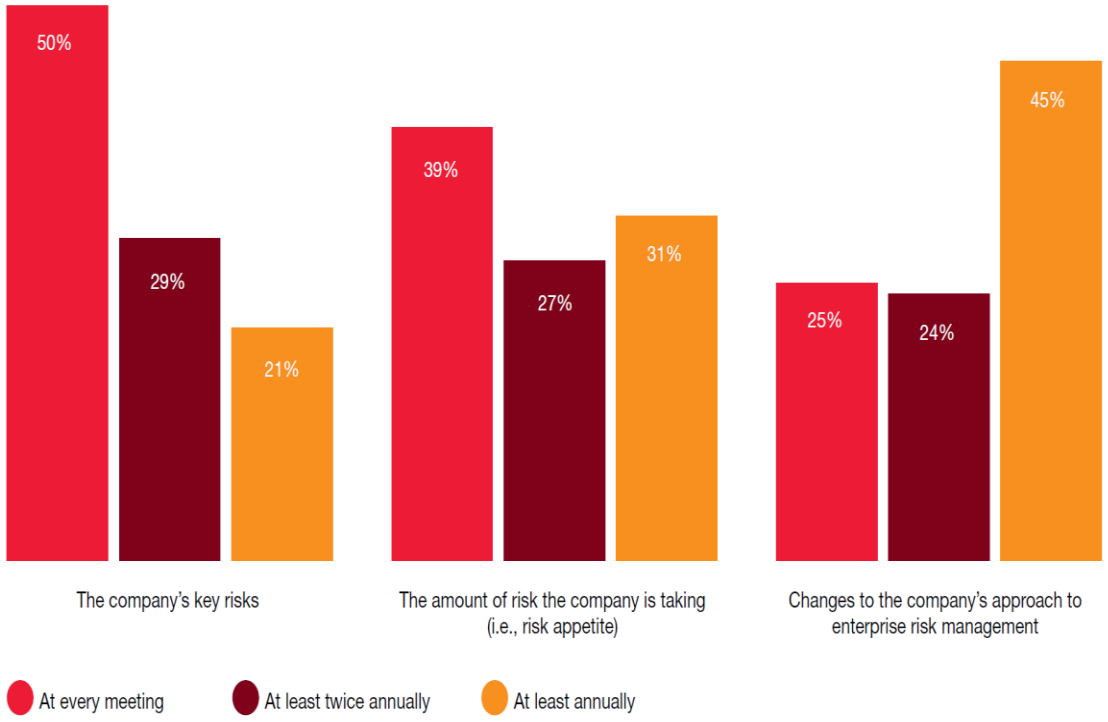


Source: *2017 PwC 20th Annual CEO Survey*

At the same time, many Boards are not receiving the information they need

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

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

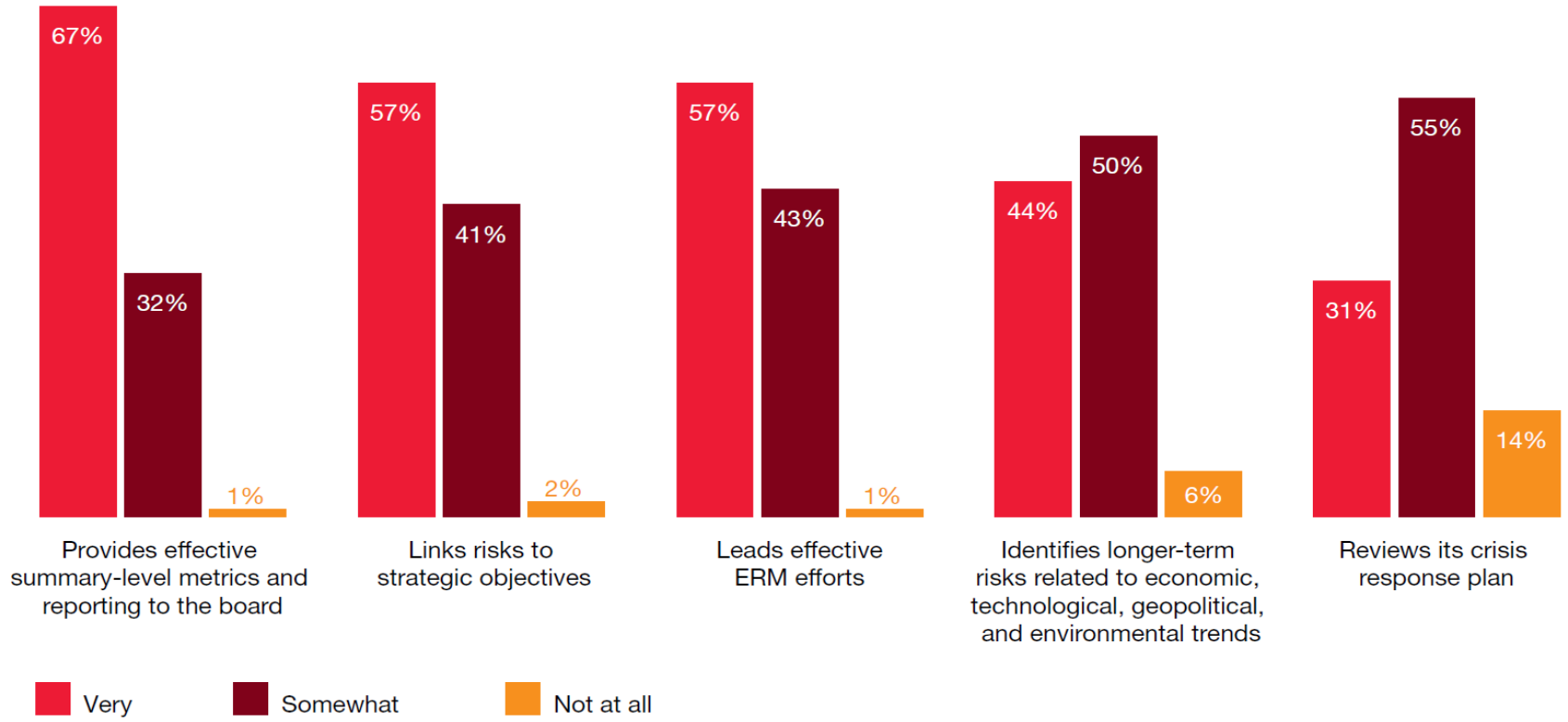


0–1% of directors responded 'Don't know';
1–6% of directors responded 'Never'

Source: PwC, *2016 Annual Corporate Directors Survey*, October 2016.

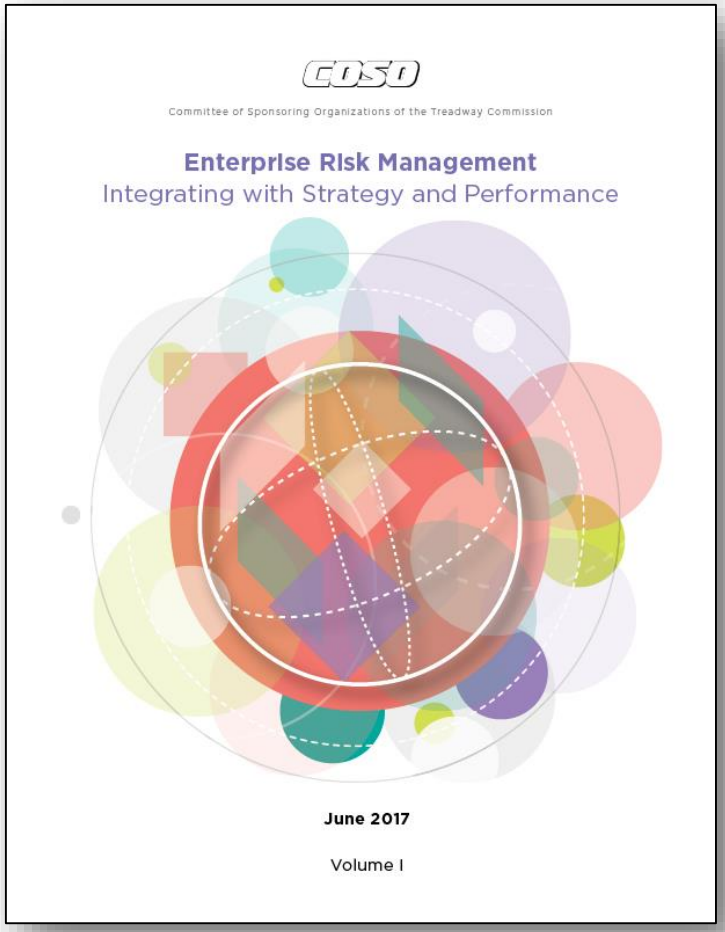
Boards recognize that there are opportunities for ERM to add greater value

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



Source: PwC, *2016 Annual Corporate Directors Survey*, October 2016.

So what are risk and business professionals saying?



Since 2004, the market has continued to evolve and the COSO Framework is evolving with it.

Why update the ERM framework now?

- **Boards are expecting more** from their organization'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**

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.

1 Website visits

Over 24,000 website visits

2 Global interest

46% of the downloads outside of the US

3 Entity interest

Wide spread interest across industry

4 Engagement

Equal interest by private & public companies

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 categorized 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 to 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, realization, and preservation of value

Written from the perspective of the business–risk management concepts are discussed in terms of helping an organization create value, enabling you to realize true benefits from ERM

Explores management of risk at all altitudes of the organization–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 organization 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 Framework

Suite of new graphics highlighting the relationship between risk and performance demonstrating a new way 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 organization'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 organization through to the creation of enhanced value.

5

Components that align to the business life cycle

20

Supporting principles that collectively describe the ERM Framework

The new Framework adopts a components and principles structure

Governance & Culture

1. Exercises Board Risk Oversight
2. Establishes Operating Structures
3. Defines Desired Culture
4. Demonstrates Commitment to Core Values
5. Attracts, Develops, and Retains Capable Individuals

Strategy & Objective-Setting

6. Analyzes Business Context
7. Defines Risk Appetite
8. Evaluates Alternative Strategies
9. Formulates Business Objectives

Performance

10. Identifies Risk
11. Assesses Severity of Risk
12. Prioritizes Risks
13. Implements Risk Responses
14. Develops Portfolio View

Review & Revision

15. Assesses Substantial Change
16. Reviews Risk and Performance
17. Pursues Improvement in Enterprise Risk Management

Information, Communication & Reporting

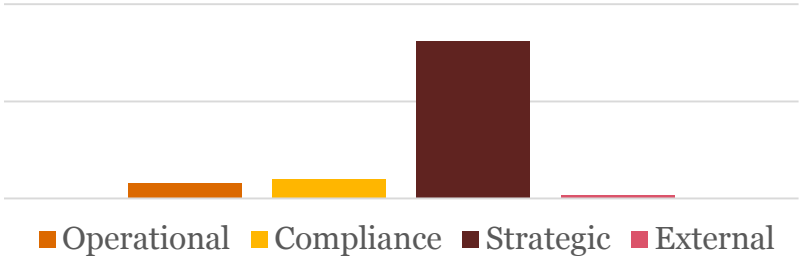
18. Leverages Information and Technology
19. Communicates Risk Information
20. Reports on Risk, Culture, and Performance

Explores the benefits of ERM

Increasing the range of opportunities	*Identify and manage risks entity-wide*	*Increasing positive outcomes*	*Reducing performance variability*	*Improving resource deployment*	*Enhancing enterprise resilience*
By considering all possibilities, both positive and negative aspects of risk, management can identify new opportunities and associated challenges	Management identifies and manages these entity-wide risks to sustain and improve performance	Improve management's ability to identify risks and establish appropriate responses, reducing surprises and related costs or losses	Management can anticipate the risks that would affect performance and put in place the actions needed to minimize disruption and maximize opportunity	Risk information enables management, in the face of finite resources, to prioritize resource deployment and enhance resource allocation	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 organizations 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 organization 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



Studies have confirmed that 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 organizations 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

Where do your ERM efforts currently focus and how closely does it align to value creation, realization and preservation?

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
3. Risk to strategy and performance

New graphics depict the alignment between risk and performance

Questions for your organization

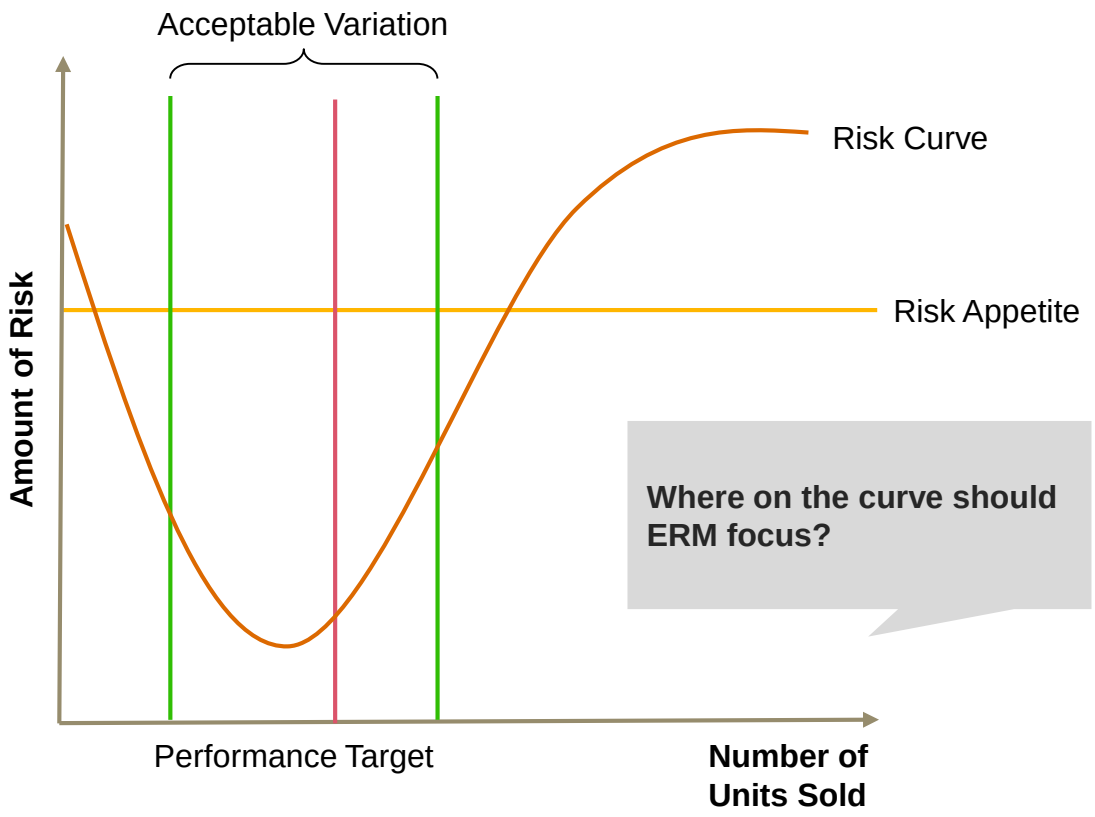
Is the risk assumed by the entity, when setting performance targets, understood?

What assumptions inform the shape of the risk curve?

Do existing key indicators demonstrate movement along the curve?

What level of performance is assumed when assessing impact and likelihood?

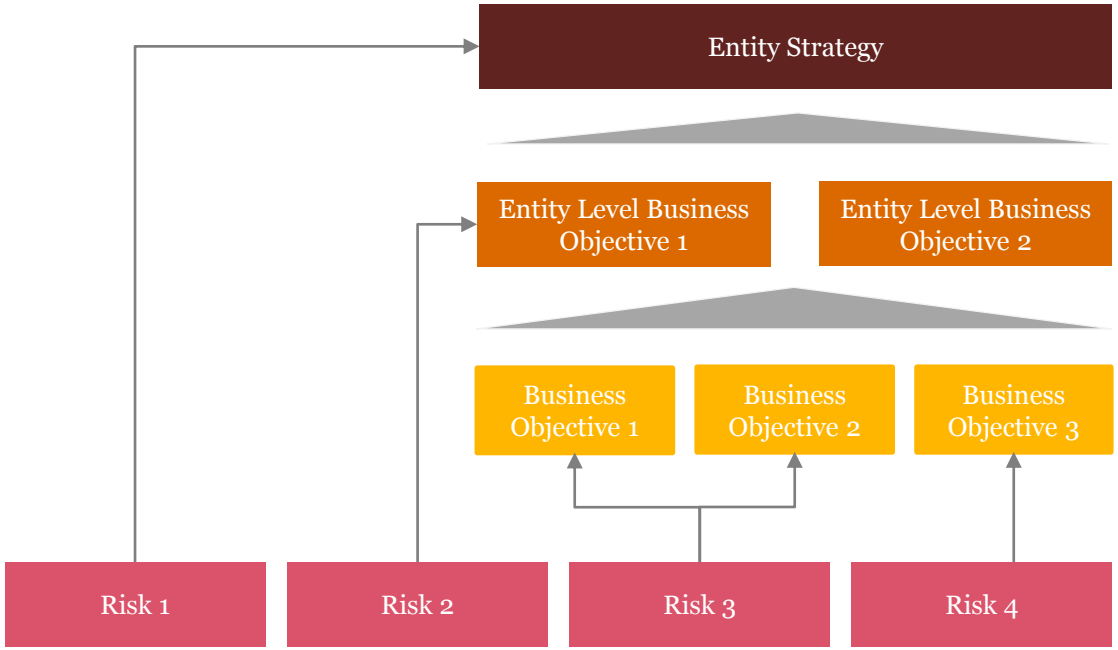
Business objective: Increase sales



Explores managing risk at all altitudes of the organization

The Framework highlights that **risks emanate and must be managed at all levels of the organization**. 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.

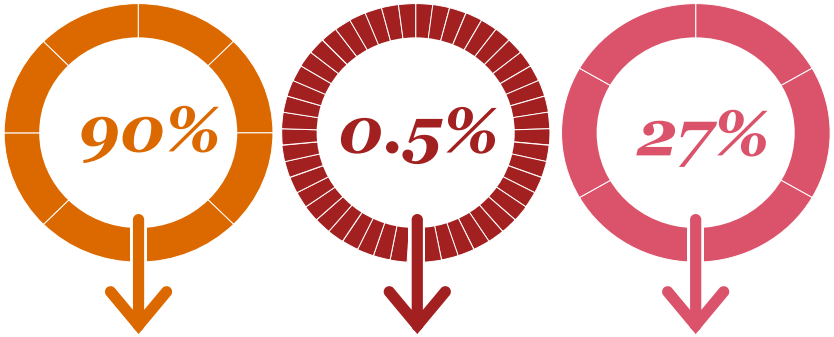
The Framework also addresses how **risks can change in severity and prioritization at different levels of the organization** and how the impacts of correlation and diversification are considered when analyzing the risk profile of portfolio view of risk.



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

How the Framework emphasizes technology

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



Data Generation

Proportion of data that exists today was created in the past two years

Data Analysis

Only a small fraction of available data is currently analyzed

Impact on Industry

Percentage of CEOs that believe technology will completely reshape their industry

Source: PwC Mega Trends – Technological Breakthroughs

- Framework emphasizes 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

Written from the perspective of the business

The framework was written from the perspective of the business to facilitate the integration of ERM and support acceptance and adoption by the business

- Research has confirmed that there is often a 'siloed' approach to risk that is separate from the day to day management of an organization
- 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 removes risk 'jargon' and adopts the language of business to discuss concepts and practices
- By using the same language, the Framework hopes to promotes acceptance and adoption of ERM by the organization

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 organization'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 organization rely on to manage risk in creating, preserving and realizing value

Discussions on the importance and commitment to integrity and ethics have been retained in the COSO Internal Control Integrated Framework

Risk Appetite

Risk Assessment and Aggregation

Portfolio View

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 a evaluative vs decision-making tool
- Alignment of risk appetite to risk assessment and the portfolio view of risk

Additional focus on:

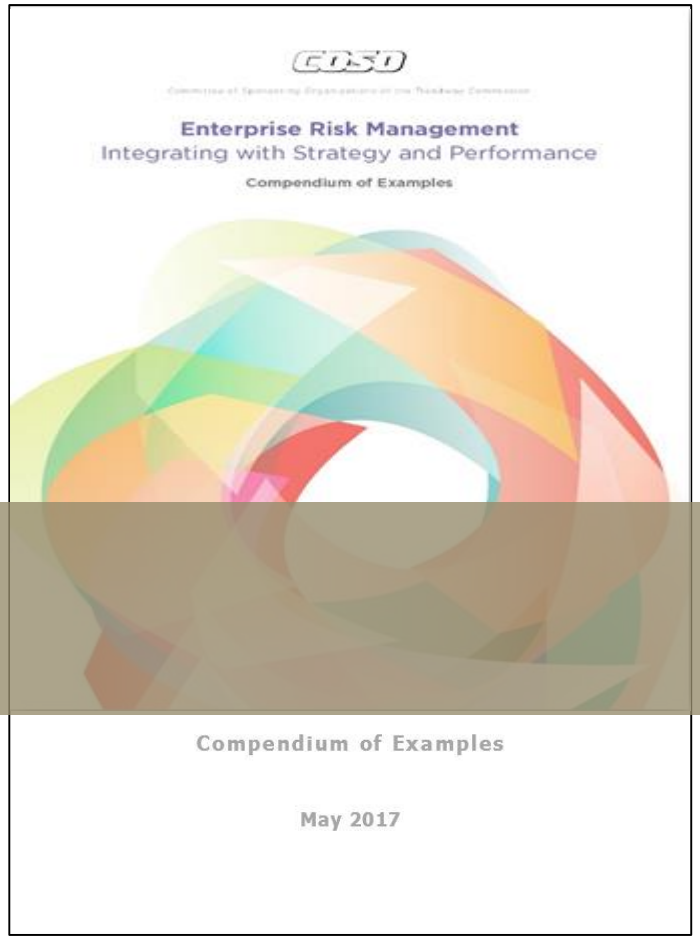
- Articulating risks relative to business objectives and performance
- Developing severity measures and prioritization criteria given the risk appetite of the organization
- Risk assessments at different levels including new illustrative graphics relating to aggregation

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

Compendium of Examples



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
- 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

www.pwc.com

More information

pwc

Staying involved

Access the Framework at www.coso.org

View videos, blogs and articles at http://www.pwc.com/us/en/risk-management/coso-erm-framework

Julien Muller
Senior manager
Tel: +33 (0)6 43 02 45 49
Julien.muller@pwc.com