The Revised COSO ERM Framework

Robert Hirth
Chairman, COSO

Instituut van
Internal Auditors
Nederland

COSO: Thought Leadership to Improve Your Organization

What the Heck is COSO?…

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management (ERM) internal control and fraud deterrence.

American Accounting Association — Thought Leaders in Accounting	9,300
AICPA American Institute of CPAs	386,000
fei Financial Executives International	15,000
ima The Association of Accountants and Financial Professionals in Business	67,000
The Institute of Internal Auditors	180,000

> 600,000

National Commission on Fraudulent Financial Reporting formed with James C. Treadway, Jr., former SEC Commissioner and General Counsel, Paine Webber as its Chairman – becoming known as the “Treadway Commission” a private-sector initiative, was formed in 1985 to inspect, analyze, and make recommendations on fraudulent corporate financial reporting.

Source: sechistorical.org

The Internal Control Recommendation

All public companies should maintain internal controls that provide reasonable assurance that fraudulent financial reporting will be prevented or subject to early detection - this is a broader concept than internal accounting controls…

…The Commission also recommends that its sponsoring organizations cooperate on developing additional, integrated guidance on internal controls…

- Treadway Commission report

Mission

COSO's Mission is "To provide **thought leadership** through the development of comprehensive frameworks and guidance on **enterprise risk management**, **internal control** and **fraud deterrence** designed to improve organizational performance and governance and to reduce the extent of fraud in organizations."

COSO's Fundamental Principle

Good risk management and internal control are necessary for long term success of all organizations

COSO is Happy !

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Recent “Situations”

Internal Control Does Matter…

February 25, 2016

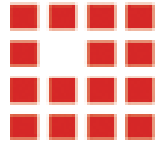
Tupperware Brands (NYSE:TUP) slides nearly 5.5% after the company said in a SEC filing it said it's still assessing deficiencies related to the information technology systems used in its financial reporting and won't file its 10k annual report on time. Instead, it expects to file its report within the 15-day extension period. "Although the Company has not concluded its assessment of the effectiveness of its internal control over financial reporting, the Company believes that these deficiencies could represent a material weakness in its internal control over financial reporting," the company said.

Tone is Critical…

…internal control over financial reporting and disclosure controls and procedures will not be effective at December 31, 2015.

The improper conduct of the company's former Chief Financial Officer and former Corporate Controller, which resulted in the provision of incorrect information to the Committee and the company's auditors, contributed to the misstatement of results. In addition, as part of this assessment of internal control over financial reporting, the company has determined that the tone at the top of the organization and the performance-based environment at the company, where challenging targets were set and achieving those targets was a key performance expectation, may have been contributing factors resulting in the company's improper revenue recognition.

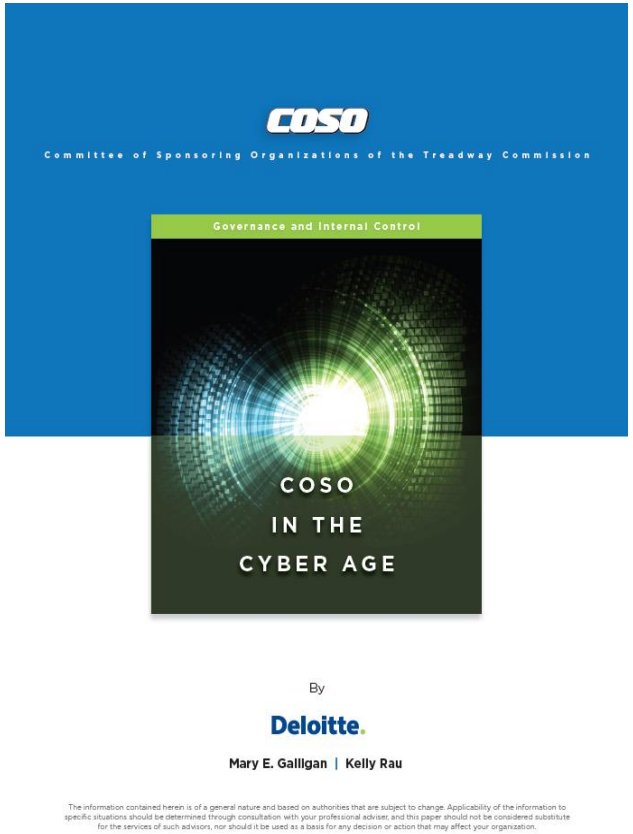
Impact on Value…



LendingClub

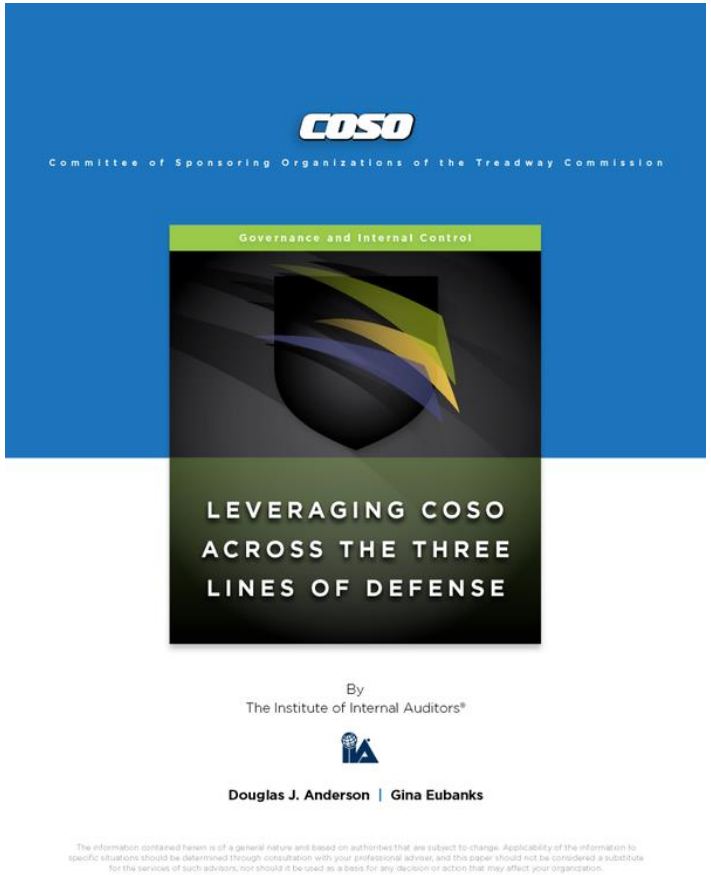
May 9 (Reuters) - Online lending platform operator Lending Club Corp said its Chief Executive and Chairman Renaud Laplanche has resigned following an internal review, which revealed a violation of the company's business practices.

- Shares of the company were down 15.6 percent at $5.99 in premarket trading.
- The review revealed that loans extended to a single investor did not conform to instructions, with certain employees being aware that the sale did not meet the investor's requirements, the company said on Monday.



COSO in the Cyber Age: Report Offers Guidance on Using Frameworks to Assess Cyber Risks

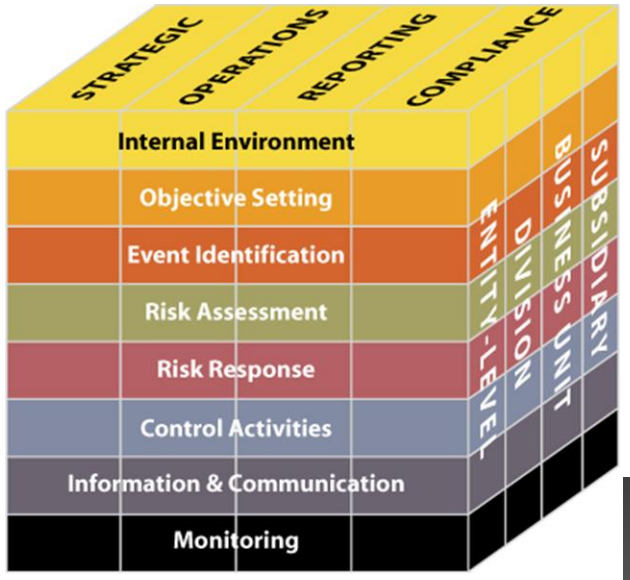
The Committee of Sponsoring Organizations of the Treadway Commission (COSO) has released COSO in the Cyber Age, a thought leadership paper that provides direction on how the Internal Control-Integrated Framework (2013) and the Enterprise Risk Management-Integrated Framework (2004) can help organizations effectively and efficiently evaluate and manage cyber risks.



Leveraging COSO Across the Three Lines of Defense:

Advocates for clearly defining responsibilities for three aspects of risk: risk ownership, risk monitoring, and risk assurance. Respectively, functions that own and manage risks are the first line. Various risk control and compliance functions that monitor risks are the second line. Internal audit, which provides independent assurance on the effectiveness of control and compliance functions, is the third line.

Our Next Challenge and Opportunity



COSO Announces Project to Update *Enterprise Risk Management- Integrated Framework…*

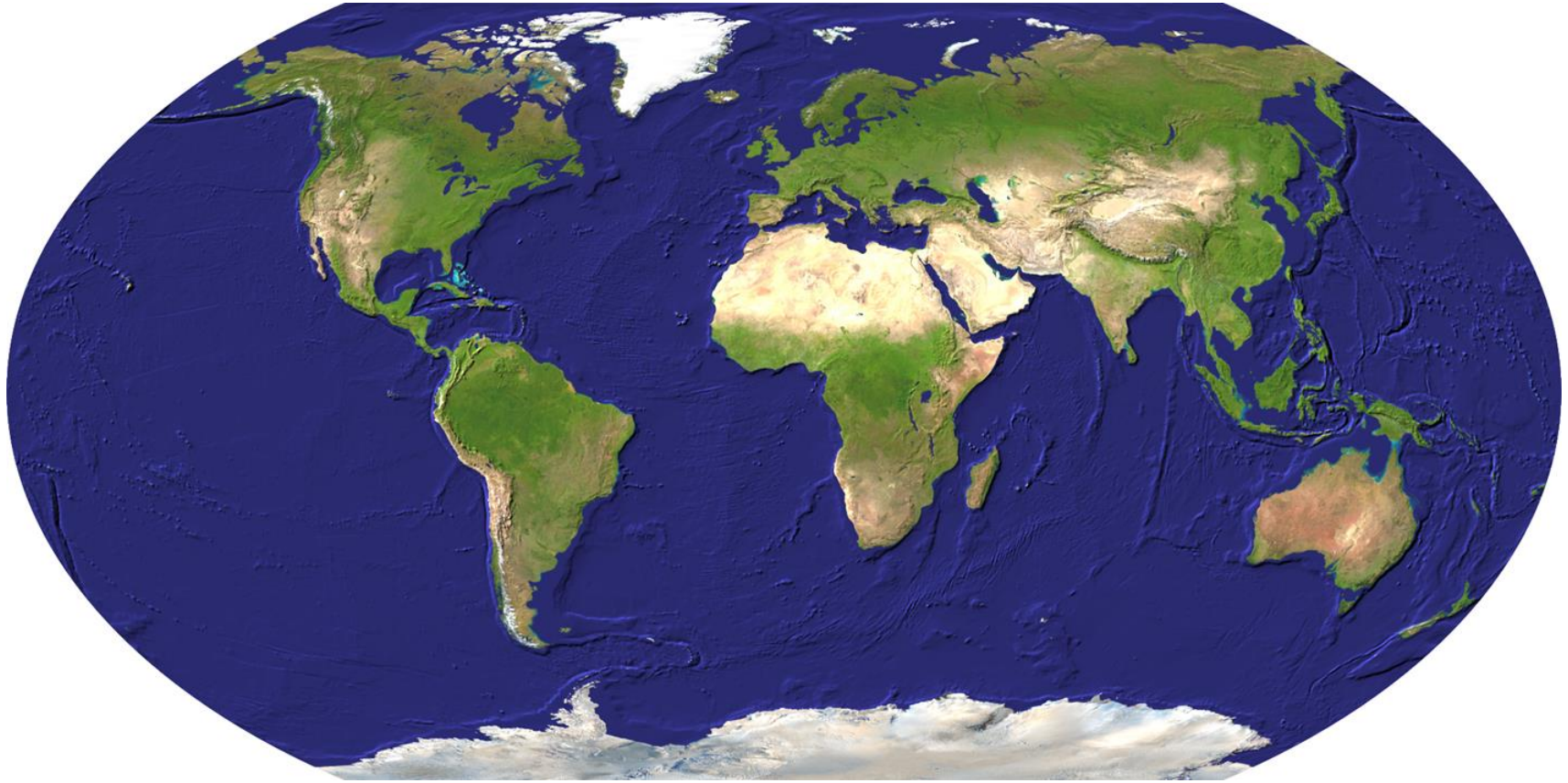
- **NEW YORK, October 21, 2014 --** The Committee of Sponsoring Organizations of the Treadway Commission (COSO) today announced a project to review and update the 2004 *Enterprise Risk Management–Integrated Framework* (Framework).
- The Framework, originally published in 2004, is a widely accepted framework used by management to enhance an organization's ability to manage uncertainty and to consider how much risk to accept as it strives to increase stakeholder value.
- This initiative is intended to enhance the Framework's content and relevance in an increasingly complex business environment **so that organizations worldwide can attain better value from their enterprise risk management programs.** The initiative also will develop tools to assist management in reporting risk information and in reviewing and assessing the application of enterprise risk management.

Why Update the Framework Now?

- Concepts and practices have evolved
- Lessons learned
- Bar raised with respect to enterprise risk management
- Business and operating environments more complex, technologically driven, and global in scale
- Stakeholders more engaged, seeking greater transparency and accountability
- Risk discussions increasingly prominent at the board level


KEEP
CALM
IT'S
COMING
SOON...

Global Interest and Application Has Increased Significantly !



SEC Proxy Requirement…

Provide Information About Board Leadership Structure and the Board's Role in Risk Oversight:

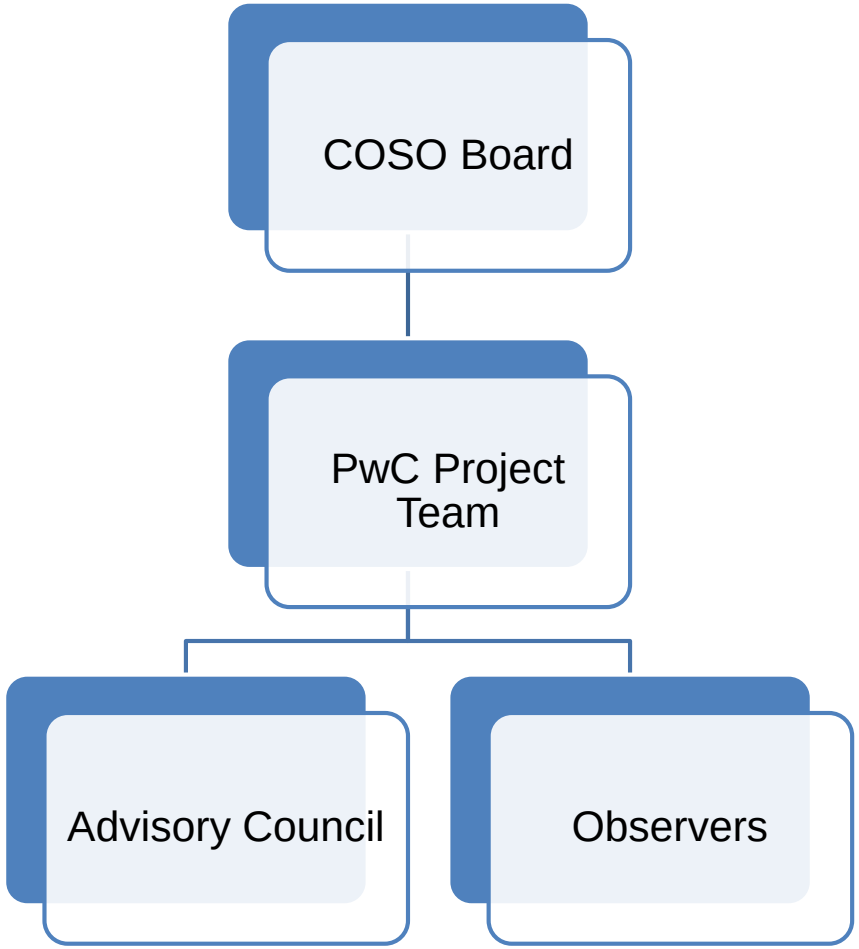
- The SEC approved rules relating to board leadership structure and the board's role in risk oversight. The rules require disclosure about:
- A company's board leadership structure, including whether the company has combined or separated the chief executive officer and chairman position, and why the company believes its structure is the most appropriate for the company at the time of the filing.
- In certain circumstances, whether and why a company has a lead independent director and the specific role of such director.
- **The extent of the board's role in the risk oversight of the company.**

TEN PRINCIPLES OF RISK OVERSIGHT

protiviti®

1. Understanding the company's key drivers of success
2. Assess the risk inherent in the strategy
3. Define the role of the full board and its standing committees with regard to risk oversight
4. Consider whether the risk management system is appropriate and sufficiently resourced
5. Understand and agree with management the types and format of risk information required
6. Encourage dynamic, constructive risk dialogue between management and the board
7. Closely monitor the potential risks in the company's culture and its incentive structure
8. Monitor critical alignments – of strategy, risk, controls compliance incentives and people
9. Consider emerging and interrelated risks: What's around the next corner?
10. Periodically assess the risk oversight process in view of the board's oversight objectives

Project Governance



Advisory Council and Observers:

- Consists of over 25 professionals
- Provides input, expertise, feedback, insight, and ideas throughout the update.
- Obtains and synthesizes feedback from their respective constituency, organization, industry

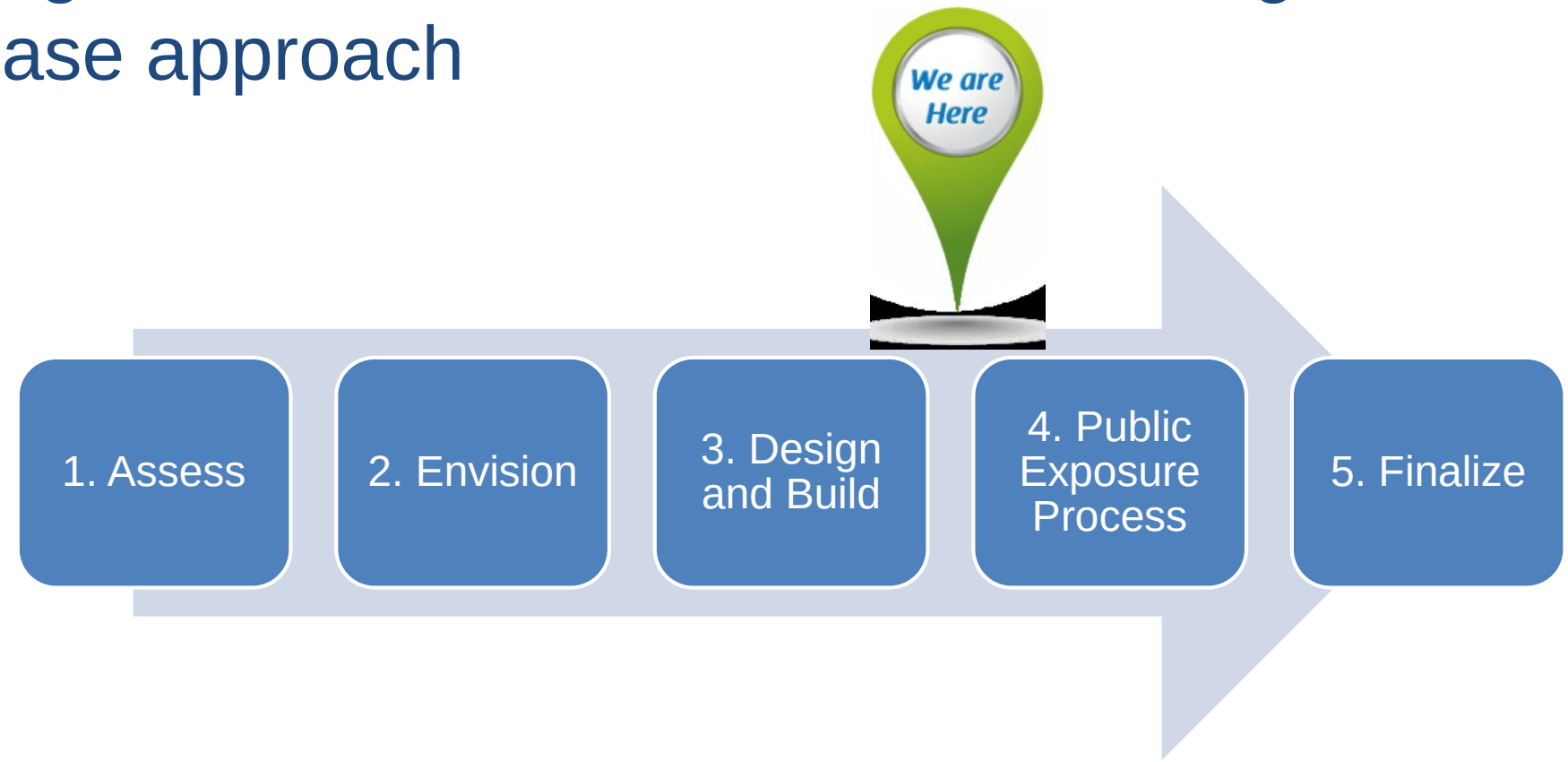
Advisory Council

- **CRO's**
- Risk Luminaries
- Risk Management, ERM University Professors
- Chief Audit Executives
- Accounting Firm Risk Practice Partners
- Board Members
- Public Sector
- Company Executives

Official Observers

- FDIC
- OIG
- GAO
- IMA
- IFAC
- RIMS
- ISACA
- China Ministry of Finance (Special)
- SEC- declined
- PCAOB determined to not be relevant given no audit requirements

Updating the Framework is undertaken using the following five phase approach



Foundational Concepts of ERM

- Every entity exists to provide value for its stakeholders
- All entities face uncertainty
- Uncertainty presents both risk and opportunity
- The challenge for management is to determine how much uncertainty to accept as it strives to grow stakeholder value
- ERM enables management to effectively manage uncertainty and associated risk and opportunity

Topics Included in the 2004 COSO ERM Framework…

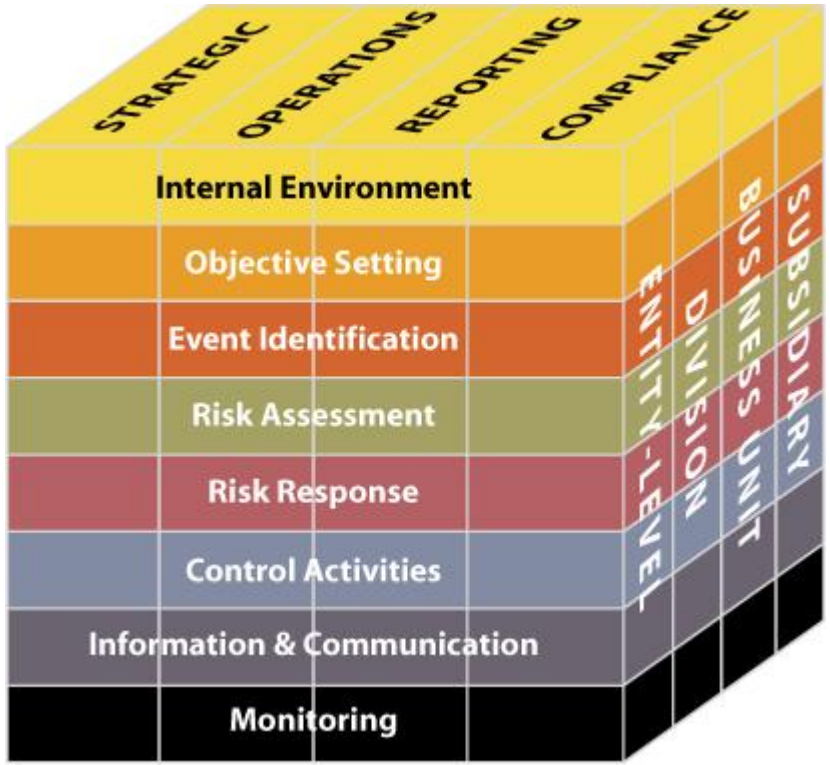
- Aligning Risk Appetite and Strategy
- Enhancing Risk Response Decisions
- Reducing Operational Surprises and Losses
- Identifying and Managing Multiple and Cross-enterprise Risks
- Seizing Opportunities
- Improving Deployment of Capital

ERM is Defined as….

"A process effected by an entity's board of directors, management and other personnel, applied in a strategic setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Key Goals

- Usefulness
- Clarity
- Value Proposition
- Relevance
- Suitability
- Effectiveness



Key Questions Helping to Inform the Update of the Framework…

1. What is your ideal view of ERM?
2. What are three strengths of the 2004 Framework?
3. What are three significant areas for update and revision?
4. What should the Framework do to stay relevant for the next 10 years?
5. What would improve user acceptance?

1. What is your ideal view of ERM?

- Baked in, embedded, not a bolt-on
- Accelerates growth and success
- Improves decision making and performance
- Discipline, not a process
- Ability to take on more risk
- Continuous, identifiable, structured

2. What are Three Strengths of the 2004 Framework?

- Linking Risk to Strategy setting
- Linkage to objectives
- Discussion of risk responses
- Linkage to internal control
- Evaluation/Attestation criteria concept
- Discussion of Board governance and oversight
- Due process

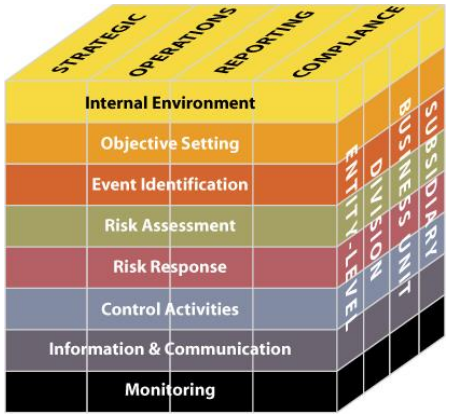
Link to Strategy…

- 85% of respondents chose strategy as their board's top focus area.
- 44% chose risk oversight as the leading issue.
- More than half (52%) said their boards discuss strategy at every board meeting.
- *"These two topics, strategy and risk oversight, go hand-in-hand as boards remain vigilant and focused on monitoring strategy and related metrics and alternatives, while also overseeing and mitigating risks to the strategy and the business itself,"*

Source: Deloitte Corporate Governance Center

Document Structure

- We anticipate that the updated Framework **will include components and principles**
  - The 2004 Framework contained over 100 key principles in an appendix. The updated Framework will significantly reduce this number
- The Project Team will also be review aspects of the update including:
  - Components
  - Categories of objectives
  - The business model



Components and Principles Structure…

Control Environment	1. Demonstrates commitment to integrity and ethical values 2. Exercises oversight responsibility 3. Establishes structure, authority and responsibility 4. Demonstrates commitment to competence 5. Enforces accountability
Risk Assessment	6. Specifies suitable objectives 7. Identifies and analyzes risk 8. Assesses fraud risk 9. Identifies and analyzes significant change
Control Activities	10. Selects and develops control activities 11. Selects and develops general controls over technology 12. Deploys through policies and procedures
Information & Communication	13. Uses relevant information 14. Communicates internally 15. Communicates externally
Monitoring Activities	16. Conducts ongoing and/or separate evaluations 17. Evaluates and communicates deficiencies

Kind of…


TOP SECRET
CONFIDENTIAL
TOP SECRET
CONFIDENTIAL
TOP SECRET

What's Likely to Stay the Same…

- Link to strategy and objectives
- An activity involving many people- Board, management and others
- Ability to cascade down to subsidiary, division, function, etc.
- Risk identification, assessment, prioritization and response
- Control activities as a possible response, link to internal control
- An ability to assess effectiveness
- Monitoring to ensure effectiveness and value of efforts
- A definitive body of knowledge and thought leadership

A Key Introduction…

"Our understanding of the nature of risk, the art and science of choice lies at the core of our modern market economy.

Every choice we make in the pursuit of objectives has its risks. From day-to-day operational decisions to the fundamental trade-offs in the boardroom, dealing with uncertainly in these choices is a part of our organizational lives."

The Strategic Value of ERM…

- Increase the range of opportunities
- Identify and manage entity-wide risks
- Reduce surprises and losses
- Reduce performance variability
- Improve resource deployment
- Anticipate, identify, adapt and respond to change

What the Update Does….

- Provides greater insight into strategy and the role of ERM when setting and executing strategy
- Enhances alignment between performance and ERM
- Accommodates expectation for governance and oversight
- Recognizes globalization and need to apply a common albeit tailored approach
- Presents new ways to view risk in setting and achieving objectives in the context of greater complexity
- Expands reporting to address greater transparency
- Accommodates evolving technology

Deeper Strategy Considerations…

- Driving ERM into the strategy setting process
- Possibility of strategy NOT ALIGNING with mission, vision and core values
- Implications FROM the strategy chosen
- Risks TO executing the strategy
- Acceptable variation in performance considerations and impact on risk

Something to Ponder…

At Your Organization:

Is risk identification, assessment and response done after strategy is formulated or is it an integral part of the strategic planning process?

In Addition…

- Explicitly addresses culture
- Anchors to Mission, Vision and Values
- Sets out core definitions, components and principles
- Direction for all levels of management involved in designing and conducting ERM activities
- Provides board and senior management overview via Executive Summary
- Accommodates different viewpoints and organizational structures
- Addresses how internal control “fits in”
- Includes over 100 clarifying examples covering a variety of industries, including public sector and non-for profit

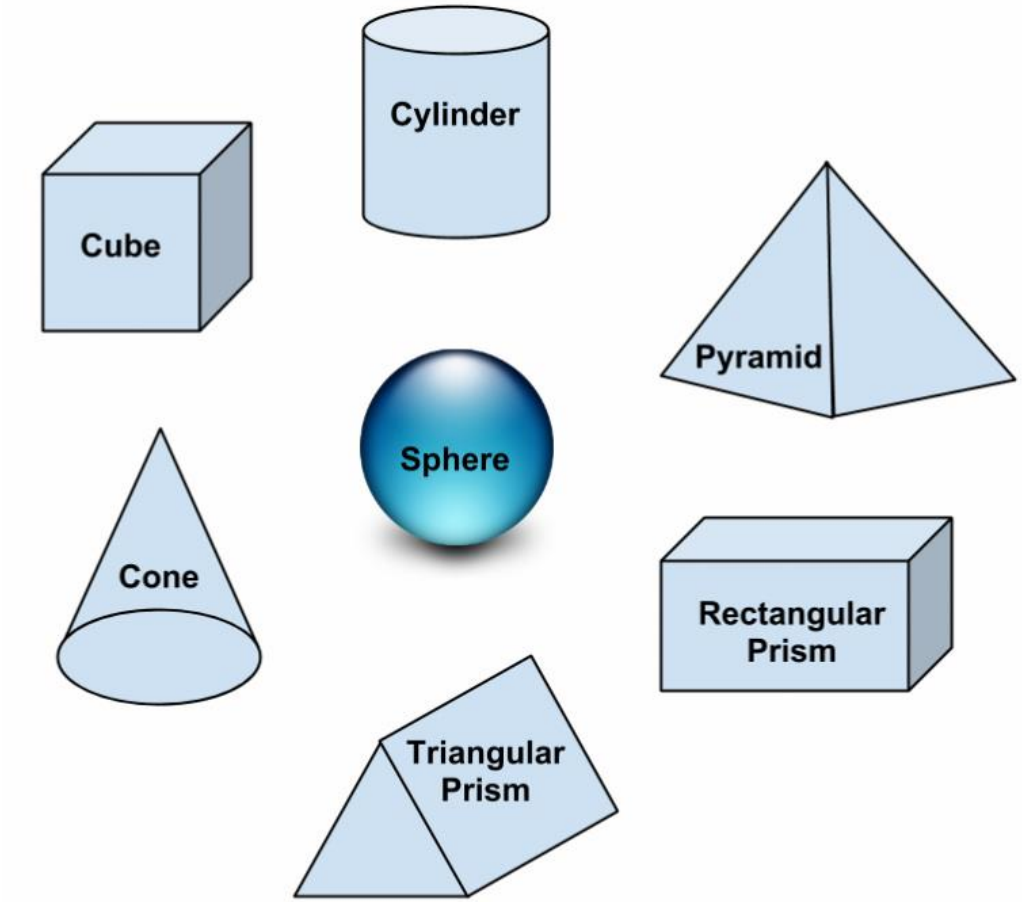
One Person's Suggestion…

"Enterprise Risk Management is an integrated discipline and activity that better enables organizations to make decisions, meet their strategic goals and achieve their mission by managing risk and seizing opportunity."

Is this a Better Definition?

"The culture, capabilities and practices integrated with strategy-setting and execution that organizations rely on to manage risk and uncertainty in creating, preserving, sustaining and realizing value."

And Maybe- A New Graphic!



Could These Be Logical Components?

- Risk Governance and Culture
- Risk, Strategy and Objective Setting
- Risk in Execution
- Risk Information, Communication and Reporting
- Monitoring Risk Management Performance

Example Principles: *Risk Information, Communication and Reporting*

- Uses Relevant Information
- Leverages Information Systems
- Communicates Risk Information
- Reports on Risk Culture and Performance

Bridging Between ERM and Internal Control Frameworks

An Enhanced View…

"ERM is a discipline and mindset **imbedded throughout an organization** which **improves decision making** in governance, strategy setting, operations, reporting and compliance. It helps to **accelerate growth and enhance performance** by **more closely linking objectives to risk** and opportunity in a more formal and structured manner which **better protects and creates organizational value**. "

Incrementalism…

“How would you like to meet more of your objectives more of the time? “

COSO Can Help ALL Organizations!

A Suitable Model Everywhere…

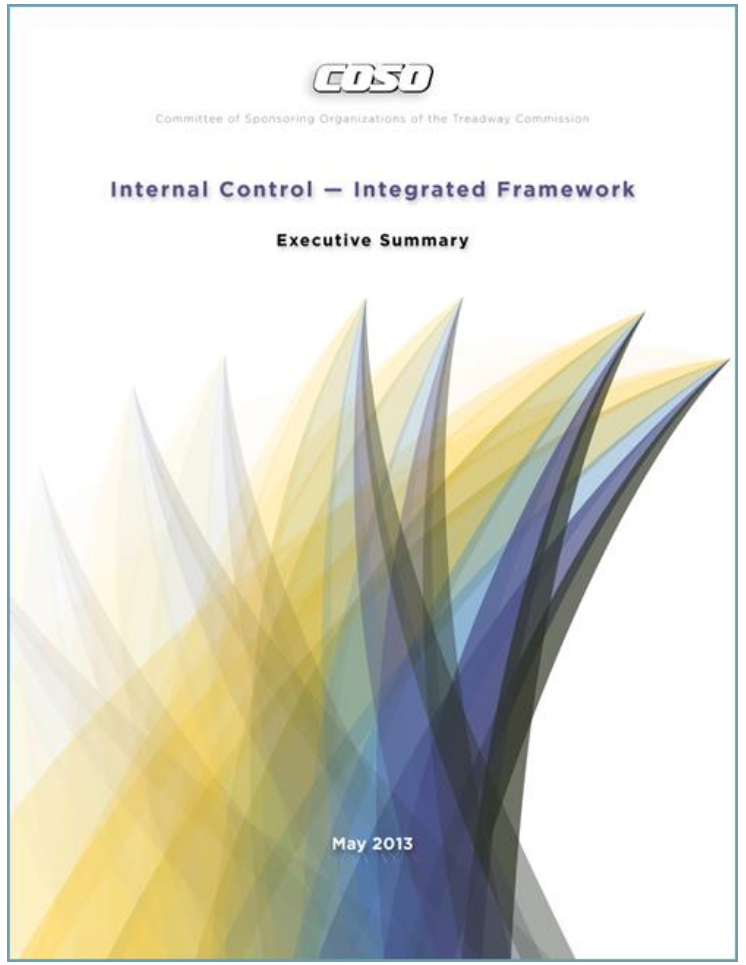
Some Key Take-Aways

- Everyone is doing ERM – can you do it better?
- Analyze, understand and communicate your strategy better
- Tie it in to Decision-making and performance, cascade it down
- Keep it moving- it's a journey
- It happens all the time- and is part of all decision-making
- You need a Tone at the Top
- Information can be leveraged
- Stay attuned to what's on the Horizon (emerging risks, change)

How to Engage with COSO and the Project Team

- Reach out to an Advisory Council member
- Participate in surveys
- Attend / organize a roundtable
- **Participate in the public exposure process**
- Connect directly via email with the PwC Project Team at: COSO-ERM_Update@us.pwc.com

Dank je !


Committee of Sponsoring Organizations of the Treadway Commission
Internal Control — Integrated Framework
Executive Summary
May 2013