Overview of Presentation

- Brief History of ERM
- Who cares about ERM
- Recent Studies
- Status of ERM Implementation (Survey Results)
- Getting Started on ERM
- Internal Audit’s Role in ERM
**Brief History of ERM**

The COSO ERM Framework has eight Components and four objectives categories. It is an expansion of the COSO Internal Control-Integrated Framework published in 1992 and amended in 1994. The eight components are:

- **NYSE corporate governance rules**
- **SEC**
  - Heightened Focus of the National Exam Program
- **Standard & Poor’s begin including an ERM assessment in its ratings for non-financial companies starting in 2009**
- **ISO 31000: Principles and Guidelines on Implementation**

In the last few years, we have seen an increased focus on ERM by the NYSE, Standard and Poor’s, the SEC and the International Organization for Standardization.
What is Enterprise Risk Management

- Enterprise-wide risk management (ERM) is a structured, consistent and continuous process across the whole organization for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.
  - THE ROLE OF INTERNAL AUDITING IN ENTERPRISE-WIDE RISK MANAGEMENT. 2009 The IIA

- “Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”
Common ERM Challenges

- Identifying executive sponsors for ERM.
- Establishing a common risk language or glossary.
- Describing the entity's risk appetite (i.e., risks it will and will not take)
- Identifying and describing the risks in (risk universe or inventory).
- Implementing a risk-ranking methodology to prioritize risks within and across functions.
- Establishing a risk committee and or Chief Risk Officer to coordinate certain activities of the risk functions.
- Establishing ownership for particular risks and responses.
- Demonstrating the cost-benefit of the risk management effort.
- Developing action plans to ensure the risks are appropriately managed.
- Developing consolidated reporting for various stakeholders.
- Monitoring the results of actions taken to mitigate risk.
- Ensuring efficient risk coverage by internal auditors, consulting teams, and other evaluating entities.
- Developing a technical ERM framework that enables secure participation by 3rd parties and remote employees.
Business Functions (Common Silos)

- Strategic planning
- Marketing
- Compliance & Ethics
- Customer service
- Internal audit
- Accounting / Financial compliance
- Legal Department
- Insurance (Risk Management)
- Treasury
- Operational Quality Assurance
- Purchasing
- Information Technology
- Operations management
- Credit
- Public Relations
- Human Resources
Who Cares About ERM

IIA
AICPA
COSO
ISO

Audit Committee & Board

SEC
PCAOB
NYSE
S&P

YOU
Some Specifics

**NYSE**

- While it is the job of the CEO and senior management to assess and manage the company’s exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee should discuss the company’s major financial risk exposures and the steps management has taken to monitor and control such exposures.

  - NYSE Listing Standards Part 7 (D)

**ISO 31000**

- This new standard is broken into three sections: Principles and Guidelines; Framework; and Process
- The IIA has issued a Practice Guide: Assessing the Adequacy of Risk Management Using ISO 31000

**Standard & Poor’s**

- Classification for ERM (insurance example)
  - Excellent
  - Strong
  - Adequate
  - Weak
- Adequate can be further described as
  - Adequate With Positive Trend
  - Adequate With Strong Risk Controls
Excerpts From SEC Keynote address March 3, 2011

- We are also focusing our exams on risk management as it pertains to corporate governance, enterprise risk management (ERM) and registrants’ internal controls. … we will generally want to understand how risk management is embedded in key business processes and decision-making at five levels: (Next Slide)

- We will incorporate a strategic dialogue of the enterprise risk management framework into our exams so we can effectively distinguish the forest from the trees and then dive into targeted exams in focused risk areas such as AML to test effectiveness.

Carlo V. di Florio Director, Office of Compliance Inspections and Examinations U.S. Securities and Exchange Commission during the Keynote address at the SIFMA Anti-Money Laundering Seminar New York, NY March 3, 2011
Excerpts From SEC Keynote address March 3, 2011

- How do the business units of an entity ensure they are taking and managing risks effectively at the product and asset class level in accordance with the risk appetite and tolerances set by the board and senior management of the whole organization?

- How are key AML and other risk management, control and compliance functions structured and resourced to ensure they are effectively embedded in the business process, while having the necessary independence, standing and authority to be effective in helping the organization identify, manage and mitigate risk?

- How is senior management ensuring effective oversight of AML risk management and embedding AML risk management together with other enterprise risk management elements in key business processes?

- How does the internal audit process independently verify and provide the board and senior management with assurance regarding the operating effectiveness of AML risk and other risk management, compliance and control functions?

- How is the board of directors (if one exists in the organization) staffed and structured to ensure it can effectively set risk parameters for AML risk and other risks, foster an effective risk management culture, oversee risk-based compensation systems and effectively oversee the risk profile of the firm?
Recent ERM Studies

Four Studies published by COSO in the past year:

- COSO 2010 Report on ERM – December 2010
- Board Risk Oversight: A Progress Report – December 2010
- Developing Key Risk Indicators to Strengthen ERM – December 2010
- Embracing Enterprise Risk Management – January 2011
Since its release in 2004, COSO’s *Enterprise Risk Management – Integrated Framework* (COSO’s ERM Framework) has been widely recognized as a respected authority on the topic of Enterprise Risk Management (ERM). However, other than anecdotal observations, COSO lacked any concrete information on the extent of its adoption within organizations or market perceptions about its usability.

To gain a sense for the extent of use, consideration, or reliance on COSO’s ERM Framework, COSO commissioned the Enterprise Risk Management Initiative at North Carolina State University to conduct a survey in summer 2010 working through the COSO sponsoring organizations. This survey was targeted to individuals who are involved in leading ERM related processes or knowledgeable about those efforts within their organization.

Responses were received from 460 individuals who answered over 24 questions in the online survey that addressed both the risk management practices of the entity for which the individual is a member of management, as well as that individual’s perceptions about the strengths and weaknesses of COSO’s ERM Framework. Key findings are summarized in the following slides:
Key Findings

- The state of ERM appears to be relatively immature. Only 28 percent of respondents describe their current stage of ERM implementation as “systematic, robust and repeatable” with regular reporting to the board. Almost 60 percent of respondents say their risk tracking is mostly informal and ad hoc or only tracked within individual silos or categories as opposed to enterprise-wide.

- There appears to be a notable level of dissatisfaction with how organizations are currently overseeing enterprise wide risks. Almost half (42.4 percent) described their organization’s level of functioning ERM processes as “very immature” or “somewhat mature.” About a third (35 percent) admit that they are “Not at All Satisfied” or are “Minimally” satisfied with the nature and extent of reporting to senior executives of key risk indicators.
Key Findings (Continued)

- Almost two-thirds of respondents note that management formally reports the entity’s top risk exposures to the board on a regularly scheduled basis; however, the form of risk oversight appears to be casual and unstructured. Just under half (44 percent) note there was either no or only minimal processes for identifying and tracking risks.

- Boards of directors, especially those on the audit committee, are placing greater expectations on management to strengthen risk oversight in the majority of organizations. That in turn is perhaps encouraging CEOs to assign more responsibility within management to strengthen risk oversight.
Key Findings (Continued)

- Almost 65 percent of respondents were fairly familiar or very familiar with COSO’s ERM Framework. Very low levels of familiarity were reported with the Joint Australia/New Zealand AS/NZ 4360-2004, the Turnbull Guidance, and the ISO standards for risk management. COSO’s ERM Framework was also the overwhelming choice as the basis for implementing ERM within the respondent’s organizations. Very few respondents indicated that they used other frameworks as the basis for designing and implementing ERM processes.

- Most believe that the COSO ERM Framework is theoretically sound, provides a common language for ERM that is widely accepted by organizations, and clearly describes key elements of a robust ERM process. There was some criticism that COSO’s ERM Framework is overly theoretical. About a quarter (26.5 percent) responded significantly or “a great deal” to the perception that the COSO ERM Framework contains overly vague guidance.
Key Findings (Continued)

- While 41 percent of respondents believe the cube depiction of the COSO ERM Framework is a very effective portrayal of the inter-relationships of the elements of ERM, an additional 26.4 percent believe the cube is unnecessarily complicated and causes negative reaction to the COSO ERM Framework.

- The majority of respondents do not appear to be familiar with Volume 2 of the COSO ERM Framework, which contains Application Techniques. For those with some familiarity, there are strong indications that there is a need for more templates and tools to help with the implementation of ERM.

- The team separately analyzed results for public companies only and found the results to be mostly similar to results for the full sample.
Survey Summary

Framework Used for ERM Guidance

- COSO’s ERM Framework: 54.6%
- No One Framework: 16.9%
- Not Applicable: 13%
- Other Framework: 5.8%
- Don’t Know: 5.1%
- ISO: 1.9%
- Turnbull Guidance: 1.7%
- Joint Australia New Zealand: 1.0%

“A refocus on the reality that risks must be taken to achieve specific return objectives may help organizational leaders realize that more intelligent and focused management of risks will serve to increase the odds that strategic goals and objectives will actually be achieved.”

Manufacturing (SIC 20-39)
Finance, Insurance, Real Estate (SIC 60-67)
Services (SIC 70-89)
not-for-Profit (SIC N/A)
State or Local Government
Wholesale/Distribution (SIC 50-51)
Retail (SIC 52-59)
Construction (SIC 70-89)
All Other Combined (none greater than 2%)

COSO 2010 Report on ERM – December 2010
The traditional approach to risk management is within silos. Each person may ‘see’ risk and respond to the risk that they see, but only within their limited perspective.
The results of a limited perspective on Enterprise Risk

I.
It was six men of Indostan
To learning much inclined,
Who went to see the Elephant
(Though all of them were blind),
That each by observation
Might satisfy his mind.

II.
The First approached the Elephant,
And happening to fall
Against his broad and sturdy side,
At once began to bawl:
"God bless me!-but the Elephant
Is very like a wall!"

III.
The Second, feeling of the tusk,
Cried: "Ho!-what have we here
So very round and smooth and sharp?
To me't is mighty clear
This wonder of an Elephant
Is very like a spear!"

IV.
The Third approached the animal,
And happening to take
The squirming trunk within his hands,
Thus boldly up and spake:
"I see," quoth he, "the Elephant
Is very like a snake!"

V.
The Fourth reached out his eager hand,
And felt about the knee.
"What most this wondrous beast is like
Is mighty plain," quoth he;
"'Tis clear enough the Elephant
Is very like a tree!"

VI.
The Fifth, who chanced to touch the ear,
Said: "E'en the blindest man
Can tell what this resembles most;"Deny the fact who can,
This marvel of an Elephant
Is very like a fan!"

VII.
The Sixth no sooner had begun
About the beast to grope,
Than, seizing on the swinging tail
That fell within his scope,
"I see," quoth he, "the Elephant
Is very like a rope!"

VIII.
And so these men of Indostan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right,
And all were in the wrong!

MORAL.
So, oft in theologic wars
The disputants, I ween,
Rail on in utter ignorance
Of what each other mean,
And prate about an Elephant
Not one of them has seen!

THE BLIND MEN AND THE ELEPHANT. A HINDOO FABLE.
by John Godfrey Saxe
An Approach Getting ERM Started

I. Keys to Success - Overarching themes to provide management with a strong foundation for an effective ERM program as they develop and tailor their specific approach to implementing ERM.

II. Initial Action Steps - Action oriented, “how to” steps to implement an initial ERM effort. These steps support development and implementation of a tailored ERM initiative.

III. Continuing ERM Implementation - Next steps to further develop and broaden the organization’s initial ERM effort.

From: Embracing Enterprise Risk Management: Practical Approaches for Getting Started. COSO January 2011
Keys to Success

Support from the Top is a Necessity
- ERM initiative must be enterprise wide and viewed as an important and strategic effort
- Support from the board of directors and senior management is needed to get the right focus, resources and attention for ERM

Build ERM Using Incremental Steps
- Identify and implement key practices to achieve immediate, tangible results
- Provide an opportunity to change and further tailor ERM processes
- Facilitate the identification and evaluation of benefits at each step

Focus Initially on a Small Number of Top Risks
- One bite at a time (i.e. strategic risks or one business unit)
- Critical success factor is to focus attention on a manageable number of key risks

Leverage Existing Resources
- Significant resource commitment including investments or outside expertise to undertake an ERM project will often be a barrier
- Most organizations start their ERM effort without any specific enabling technology or automated tools
Keys to Success (Continued)

Build on Existing Risk Management Activities

- Any organization with current operations has some form of risk management activities or risk related activities already in place.
- Use communication to drive toward common risk definitions and ERM framework

Embed ERM into the Business Fabric of the Organization

- The comprehensive nature of the ERM process and its pervasiveness across the organization and its people provides the basis for its effectiveness

Provide Ongoing ERM Updates and Continuing Education for Directors and Senior Management

- ERM practices, processes and information continue to evolve
- Changes in processes, people and technology drive the need for continuing education around ERM in your organization

Get Started
Just DO IT

- No time like the present
- Incremental progress is key
Initial Action Steps

Seek Board and Senior Management Leadership, Involvement and Oversight

Select a Strong Leader to Drive the ERM Initiative

Establish a Management Risk Committee or Working Group

Conduct the Initial Enterprise-wide Risk Assessment & Develop an Action Plan

Inventory the Existing Risk Management Practices

Develop Your Initial Risk Reporting

Develop the Next Phase of Action Plans & Ongoing Communications
## Continuing ERM Implementation

| **A program of continuing ERM education for directors and executives** |
| **ERM education and training for business-unit management** |
| **Policies and action plans to embed ERM processes into the organization’s functional units such as procurement, IT, or supply chain units** |
| **Continuing communications across the organization on risk and risk management processes and expectations** |
| **Development and communication of a risk management philosophy for the organization** |
| **Identification of targeted benefits to be achieved by the next step of ERM deployment** |
| **Development of board and corporate policies and practices for ERM** |
| **Further discussion and articulation of a risk appetite for the organization and/or significant business units, including quantification** |
| **Establishment of clear linkage between strategic planning and risk management** |
| **Integration of risk management processes into an organization’s annual planning and budgeting processes** |
| **Expansion of the risk assessment process to include assessments of both inherent and residual levels of risk** |
| **Exploration of the need for a dedicated Chief Risk Officer or ERM functional unit** |
Internal Audit’s Role in ERM

January 2009 IIA Position Paper

THE ROLE OF INTERNAL AUDITING IN ENTERPRISE-WIDE RISK MANAGEMENT

- Categorizes the roles in ERM into the following categories
  - Core internal audit Roles in regard to ERM
  - Legitimate internal audit roles with safeguards
  - Role internal audit should not undertake
Internal Audit ERM Activities

Core
- These are activities that are aligned to providing assurance on the Enterprise Risk Management activities of the organization
- “An internal audit activity complying with the International Standards for the Professional Practice of Internal Auditing can and should perform at least some of these activities”

Legit
- These are activities that are aligned to providing consulting assistance to the organizations Enterprise Risk Management activities
- Appropriate safeguards that are required to ensure that Internal Audit independence and objectivity are maintained.

Don’t
- These activities would impair Internal Audit’s ability to provide independent and objective assurance to the audit committee
- Management is responsible for establishing and operating the risk management framework on behalf of the board.
CORE Internal Audit Roles in ERM

Assurance Activities

- Giving assurance on the risk management processes
- Giving assurance that risks are correctly evaluated
- Evaluating the risk management processes
- Evaluating the reporting of key risks
- Reviewing the management of key risks
Consulting Activities

- Facilitating identification & evaluation of risks
- Coaching management in responding to risks
- Coordinating ERM activities
- Consolidated reporting on risks
- Maintaining & developing the ERM framework
- Championing establishment of ERM
- Developing RM strategy for board approval
Safeguards in Internal Audit Consulting for ERM

Safeguards

- It should be clear that management remains responsible for risk management.
- The nature of internal auditor’s responsibilities should be documented in the internal audit charter and approved by the audit committee.
- Internal auditing should not manage any of the risks on behalf of management.
- Internal auditing should provide advice, challenge and support to management’s decision making, as opposed to taking risk management decisions themselves.
- Internal auditing cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.
- Any work beyond the assurance activities should be recognized as a consulting engagement and the implementation standards related to such engagements should be followed.
Non-Internal Audit Roles in ERM

Non-IA Activities

- Setting the risk appetite
- Imposing risk management processes
- Management assurance on risks
- Taking decisions on risk responses
- Implementing risk responses on management’s behalf
- Accountability for Risk Management
Summary – Internal Audit’s Role in ERM

- Management is responsible for establishing and operating the risk management framework on behalf of the board.

- Internal auditor’s core role in relation to ERM should be to provide assurance to management and to the board on the effectiveness of risk management. When internal auditing extends its activities beyond this core role, it should apply certain safeguards, including treating the engagements as consulting services and, therefore, applying all relevant Standards.

- Internal audit must protect its independence and the objectivity of its assurance services.

- Proper involvement of Internal Audit in ERM can help raise the profile and increase the effectiveness of internal auditing.
Questions?

For more information please contact:

John Harris CIA, CPA, CFE
Director, Risk Advisory Services
Jefferson Wells
Houston Office
1001 Fannin #600
Houston, TX 77002
(713-470-9521)

www.jeffersonwells.com