Recent Developments in Enterprise Risk Management

Dallas IIA Chapter Pre-Meeting
September 4, 2008
Agenda

- Establish a common working definition
- Update on ERM in the market (It’s here to stay…)
- Approach to setting the foundation for ERM
- Roles an IA function should (and should not) play in developing an ERM process
- Critical success factors for your organization
Establish a Common Working Definition
The Problem Every Organization Faces…

- Changes in the Operating Environment
- Risk
- Time
- Exposure to Risk
- Risk Appetite
- Strategic Management choices and actions
- Tactical activities to reduce exposure to acceptable level
- Comprehensive and Holistic Risk Management

2008

Existing Risk Management Activities

2011

Exposure to Risk

CHANGES IN THE OPERATING ENVIRONMENT

Risk Appetite

© 2008 Protiviti Inc.
This document is for your company’s internal use only and may not be distributed to any other third party.
The framework provides:

- A definition of risk and enterprise risk management; common language
- Concepts, categories, principles and other elements of a comprehensive risk management framework
- Direction for enhancing risk management
- Criteria for determining risk management effectiveness.

The COSO ERM Framework
ERM is defined by COSO as:

- A process,
- Effected by all of the entity’s personnel including the board of directors and management
- Applied across the enterprise and in strategy-setting,
- Designed to identify potential events that may effect the entity, and manage risk,
- To provide reasonable assurance regarding the achievement of entity objectives.

We believe that ERM is about establishing the oversight, control and discipline to drive continuous improvement of an entity’s risk management capabilities in a constantly changing operating environment.
What is ERM?

Companies implement ERM to:

- Reduce unacceptable performance variability
- Align and integrate varying views of risk and risk management
- Build confidence of investment community and stakeholders
- Enhance corporate governance
- Successfully respond to changing business environment
- Better allocate resources to optimize risk mitigation

Companies have different objectives, strategies, structure, culture, risk appetite and financial wherewithal; therefore, no two ERM solutions are alike
Update on ERM in the Market
ERM’s Evolution

The first versions have basic functionality…

…and people wonder if it’s really going to stick around….
Then functionality evolves…

…and people decide, “I want that!”
So everyone expects to jump directly to the future, without getting the basics down first…

…which is when people get frustrated and say, “It can’t be done at my company.”
Almost **HALF** of large companies (47%), by their own admission, consider themselves not very effective at managing their risks.

- *2007 Protiviti Risk Barometer*

About a third of directors do not understand the organization’s major risks; non-financial risk only receives “anecdotal treatment” in the boardroom.

- *McKinsey Research*

“Its (the ERM rating analysis) value will be incremental in most cases, negligible in a few, and eye-opening in some others.”

- *Standard & Poors*

“We expect to tailor the ERM analysis based on a firm's unique risks, structure, and culture. ERM is different in each sector, because the risks and necessary risk-control measures are different.”

- *Standard & Poors*
Profiles of Leading Companies

• 53% of organizations are “Very Effective” at identifying and managing all potentially significant risks

• Increase from 2006 U.S. Risk Barometer (38%)

• Yet 47% rate themselves less than “Very Effective”

• “Very Effective” companies have implemented a more sophisticated risk management infrastructure

Source: 2007 Protiviti Risk Barometer
Leading Companies Are More Likely to...

- Rigorously deploy across the company:
  - A formal risk management policy
  - A formal risk assessment process
  - A risk monitoring and reporting process
- Formally integrate their risk assessment processes and their responses to key risks with their business planning and strategy-setting processes
- Quantify their risks to a greater extent
- Report that they are on track with regard to evaluating their risk profile

These practices provide a blueprint for starting the implementation of ERM

Source: 2007 Protiviti Risk Barometer
### Top Five Perceived Benefits Arising from Risk Management Capabilities

<table>
<thead>
<tr>
<th></th>
<th>2006</th>
<th>2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Lower insurance premiums</td>
<td>Quicker identification of risk</td>
</tr>
<tr>
<td>2.</td>
<td>Quicker identification of risk</td>
<td>Better risk information and measures</td>
</tr>
<tr>
<td>3.</td>
<td>Improvements in process performance</td>
<td>Improvements in process performance</td>
</tr>
<tr>
<td>4.</td>
<td>Increased risk awareness</td>
<td>Increased risk awareness</td>
</tr>
<tr>
<td>5.</td>
<td>Better risk information and measures</td>
<td>More effective resource allocation</td>
</tr>
</tbody>
</table>

*Source: 2007 Protiviti Risk Barometer*
So What Does it all Mean?

- ERM is here to stay

- The recent focus on incorporating ERM into credit rating agency evaluation criteria is forcing the discussion at many companies

- The need to meet regulatory & market demands, improve corporate governance and enhance decision making remain common drivers for ERM

- Organizations are at varying levels of ERM maturity

- Companies recognize the need to be doing more – but are still unsure of where to start

- There is an unmet demand for simple, practical ERM guidance
Approach to Setting The Foundation
Protiviti’s ERM Methodology

The three most important things to keep in mind when implementing ERM are:

• Leverage what you are currently doing
• Integrate with your existing processes and initiatives
• Keep it simple!
Building Capabilities

Enhance Capabilities

Build Capabilities

Set Foundation

Related ERM Infrastructure Elements

- Alignment of organizational culture with acceptable levels of risk (risk appetite)
- Integration of risk responses with strategy setting and business unit operating plans
- Refine risk metrics and build risk tolerance levels for key risks
- Share best practices and promote continuous improvement across organization
- Proprietary tools to portray a portfolio view of risk
- Evaluation of risk responses and risk ownership for select high risks
- Methods/tools to collect and aggregate risk data
- Link risks to available metrics, and develop new metrics to track high risks Executive, Board and other risk reporting
- Training, awareness and communication protocols

Enterprise-wide risk assessment process
- Common risk language and definitions (risk universe)
- Steering Committee, Risk Committees or other oversight team
- Define roles and responsibilities
- Understand key management processes for integration
How IA Can Help Set the Foundation

In many cases, Internal Audit may have already developed the starting point for many of the foundational elements of ERM.

**Elements of Setting the Foundation:**

- Enterprise-wide risk assessment process
- Common risk language and definitions (risk universe)
- Steering Committee, Risk Committees or other oversight team
- Define roles and responsibilities
- Understand key management processes for integration
Enterprise Risk Assessment Approach

- **Internal Environment and Objectives**: Understand the business and its objectives.
- **Event Identification**: Identify events that negatively impact one or more business objectives.
- **Risk Assessment**: Understand, evaluate, and prioritize business risks by evaluating the impact and likelihood of potential events and existing activities.
- **Risk Response Planning**: Develop a plan to respond to high priority risks.

**Project Management / Knowledge Building / Reporting**
Case Study: Enterprise Risk Assessment

Case Background:

- Fortune 50 Retailer operating over 1300 stores with annual sales over $45 billion

- Wanted to implement an Enterprise Risk Management (ERM) process to improve company’s ability to proactively manage risks

- Key stakeholders: CFO, Treasurer, Strategic Planning, SOX, Internal Audit, Business Process Improvement
Case Study (Cont’d)

Approach:

- **Understand Objectives**
  - Gathered client IA & strategic planning documents

- **Risk identification**
  - Developed common risk language
  - Performed 15 executive level risk interviews
  - Identified over 50 risk scenarios

- **Risk Assessment**
  - Identified top 15 risks to objectives
  - Facilitated a 4 hour risk assessment session with company executives
  - The facilitated risk assessment session identified two high priority risks for further risk mitigation work
Overall Project Benefits:

- Refined common risk language and risk assessment criteria
- Developed consensus view of organization's highest priority risk
- Developed approach to consistently improve management of high priority risks
- Improved allocation of company resources, including IA plan
- Developed roadmap for integrating ERM into existing risk management activities
Roles IA Should and Should NOT Play
In line with the IIA’s guidance…

- Internal auditors DO NOT have primary responsibility for ERM implementation or maintenance.

- Acceptable roles:
  - Educator
  - Facilitator
  - Coordinator
  - Integrator
  - Evaluator
Overview of Internal Audit’s ERM Roles

This diagram is taken from “Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management”, reproduced with the permission of the Institute of Internal Auditors – UK and Ireland. For the full Statement visit www.iia.org.uk.

© The Institute of Internal Auditors – UK and Ireland Ltd, July 2004

© 2008 Protiviti Inc.
This document is for your company’s internal use only and may not be distributed to any other third party.
Overview of Internal Audit’s ERM Roles

Core internal audit roles in regard to ERM

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

Legitimate internal audit roles with safeguards

- Facilitating evaluation and identification 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

Roles internal audit should not undertake

- Accountability for risk management
- Setting the risk appetite
- Imposing risk management processes
- Management assurance on risks
- Taking decisions on risk responses
- Implementing risk responses on management’s behalf
ERM Critical Success Factors

Four key factors lead to successful implementation of ERM:

- Continuous Process Improvement
- Executive Leadership
- Enabling Frameworks
- Ownership and Commitment

Enterprise Risk Assessment Process
- Risk Management Performance Monitoring
- Best Practices For Managing Risk
- Continuous Employee Learning

Top Management Commitment and Priority
- Shared Risk Management Vision
- Compelling Business Case
- Realistic Goals
- Action Plan For Change
- Timely Management Checkpoints

Accountability For Results
- Stakeholder Involvement
- Effective Change Enablement
- Align Performance Measures
- Cultural Integration

Risk Model
- Process Classification Scheme
- Six Elements of Infrastructure

Capability Maturity Continuum
Closing Thoughts

- Don’t give up – the drivers for ERM are here to stay
- In many cases, IA can provide important input into the foundational development of an ERM process
- Leverage off existing risk management practices
- Remember the importance of culture, education and change management
"Yes, but what if the world is destroyed by asteroids and falls into the sun? What will we do then?"

"This isn't in our plan."
Questions?
Thank You & Contact Information

Charles Westrin
Manager

1125 17th Street
Suite 825
Denver, CO 80202

Phone: 720.264.2949

Charles.Westrin@protiviti.com