

Enterprise Risk Management -2010

- A Summary of the Current Status
 - The Wortham Role and Solutions to Facilitate Implementation
-

Introduction

In recent years, Enterprise Risk Management (ERM) has become an increasingly visible and important management issue. What was once considered a “best practices” program used by a few companies is now a discipline exercised by a majority of U.S. public companies and its use is expanding rapidly.

ERM broadens the scope of risk management to include every significant business risk of the organization, not just insurable risks – the historical responsibility of most risk managers. These other risks may include operational risks, market risks, credit risk, and such risks as those in long-term strategic planning, and in human capital. ERM requires that all of these risks be considered relative to each other, and to create a consolidated and consistent risk profile and practice – a portfolio view of risk.

So why has this risk analysis and management process known as ERM become so important? It should be recognized that all business organizations, even non-profits, exist to realize value for their stakeholders. That value is created, preserved, or eroded by management decisions in all activities, ranging from development of business strategies to operating the enterprise day-to-day. There are obviously many types of risks inherent in these activities and ERM can protect the value of the enterprise by enabling management to deal effectively with the potential future events that create risk, and to respond in a manner that reduces the likelihood of negative outcomes while increasing the potential for success.

Also, the risk management processes of U.S. companies are under increasing regulatory and rating agency scrutiny. The process for the management of risk exposures has also become a public disclosure issue and a significant corporate governance issue. Boards of directors are under increasing pressure to take responsibility for risk mitigation planning and oversight.

This paper will outline the basics of ERM as it has evolved over the last decade, and will discuss a number of the important issues that have driven its use by more and more companies. The paper will also describe the role that Wortham can take in the ERM implementation process.

Enterprise Risk Management 101

The practice of Enterprise Risk Management can be described as a multi-step process that includes: 1) Establishing the objectives for risk management, 2) Identifying the potential risks that may affect an entity, 3) Assessing these risks in terms of frequency and severity, 4) Developing the response to risks, 5) Managing the risk tolerance levels through the organization, 6) Communication of any inconsistencies with standards, and 7) Monitoring the risk exposure. These activities are further described below:

Developing Risk Management Objectives

- A high level view of the risk tolerance of the entity, that is, the risks that senior management and the board of directors are willing to take
- Assists in sensitizing management to risk management issues and the further development of ERM

Risk Identification

- Addresses how internal and external factors combine and interact to influence the risk profile.
- Identify potential events or activities that may have a negative impact on the achievement of objectives
- Identify events or opportunities that have a positive impact and that could be natural offsets to the negative events

Risk Assessment

- Uses a combination of both qualitative and quantitative risk assessment methodologies
- Assesses and measures risk from the perspectives of frequency and severity

Risk Response

- Identify and evaluate possible responses to risk, for instance the cost vs. benefit of risk responses and the degree to which the response might reduce the severity or the frequency of the risk
- May be used to immediately reduce or eliminate certain risks

Risk Management Activities

- Sets the policies and procedures that help ensure that the entities' activities do not vary from the established risk tolerance levels
- Established throughout the organization, at all levels and in all functions

Communication of Inconsistencies with Standards

- Provides a system that informs management of the success or failure of the control activities
- The communication system should provide pertinent information in a form and timeframe that enables people to carry out their responsibilities and to respond to any risk control issues.

Monitoring Risk Exposure

- The effectiveness of the ERM framework should be observed on an ongoing basis
- This monitoring function must be incorporated with the communication function to provide an effective management tool

The implementation of ERM can be a very challenging endeavor as the success is dependent upon very broad acceptance and usage within the business organization. It is highly critical to have sponsorship from senior management and the board. Typical challenges to implementation of ERM include:

- Ascertaining the entity's risk tolerance level for all risks
- Developing the "risk inventory"
- Implementing a risk measurement/ranking methodology
- Establishing ownership of risks
- Demonstrating the cost/benefit of the ERM project
- Developing the action plan to manage the risks
- Developing the monitoring/communication framework

While the implementation of ERM can be very challenging, the benefits to the organization should include:

Enhanced Risk Awareness:

- Holistic view of risk
- Increased visibility of risk

Improved Risk Governance:

- Better defined responsibilities
- Forums for dialogue on risk

Risk management coordination:

- Improved risk reporting
- Proactive responses to risk

Regulatory Bodies and other Organizations Impacting the Evolution of ERM

There is no question that the risk management processes of U.S. corporations are under increasing regulatory, rating agency, and stakeholder scrutiny. This increase in scrutiny has increased significantly over the last several years with the primary developments outlined below:

Sarbanes-Oxley Requirements

The Sarbanes-Oxley Act of 2002 followed a period of highly publicized accounting irregularities among U.S. corporations and the Act requires that U.S. publicly-traded corporations utilize a specific control framework in their internal control assessments. Over time, many entities have adopted the COSO Internal Control Framework (described below), which includes a risk assessment element.

The COSO Internal Control Framework

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was established in 1985 as a voluntary private-sector organization by the major professional accounting organizations in the U.S. The purpose of COSO is to provide guidance to executive management and governance entities on internal control, organizational governance, ethics, risk management, fraud, and financial reporting. In the 1990s COSO issued the report *Internal Control – Integrated Framework* to help businesses assess and enhance their internal control systems. In 2001 COSO initiated a project, and engaged PricewaterhouseCoopers, to develop a framework to effectively identify, assess, and manage risk. The report *Enterprise Risk Management – Integrated Framework* expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management.

The widely used depiction of enterprise risk management from the COSO report is shown on the following page. This model uses the components of ERM outlined in the preceding section of this paper, along with the entity's units in the vertical columns, and the four categories of objectives – strategic, operations, reporting, and compliance in the third dimension. This depiction portrays the ability to focus on the entirety of an entity's enterprise risk management, and the interconnectivity of the component subjects, the objectives, and the sub-units of the entity.



[NYSE Corporate Governance Rules and the SEC](#)

The New York Stock Exchange requires the Audit Committees of each of its listed companies to discuss policies with respect to risk assessment and risk management. The NYSE has stated “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 risk exposures and the steps management has taken to monitor and control such exposures. The Audit Committee is not required to be the sole body responsible for risk assessment and management, but, as stated above, the committee must discuss guidelines and policies to govern the process by which risk assessment and management is undertaken.”

The Securities and Exchange Commission weighed in on the appropriateness of enterprise risk management in assessing and managing risk in business organizations by requesting that public companies use information developed from ERM in the Management’s Discussion and Analysis Sections in public financial statement filings. Also, in February 2010 the SEC implemented new proxy rules that include requirements that public companies disclose compensation practices that can create material risks, and requires the disclosure of the role of the Board in risk management oversight.

Rating Agencies

A recent driver of interest in the ERM process is the increasing involvement of the rating agencies in this topic. Standard & Poor's led the way with ERM criteria initially used in the ratings of insurance and other financial industry companies, formalizing these evaluations in 2005. In April 2006 S&P decided to begin a pilot program aimed at energy companies, and over a year-long period evaluated the trading risk management programs at 10 energy firms.

In May 2008 S&P announced that it would begin an ERM assessment for virtually all rated firms beginning in 2009. This project involves discussions as a part of the regularly scheduled rating review meetings to gather information on how companies have assumed risks and why they are then comfortable with their risk positions. This discussion phase is part of a staggered implementation that will eventually result in formal scoring beginning in 2009, once sufficient and reliable benchmarking information is available.

S&P is examining two broad areas – risk management culture and strategic risk management. Risk management culture concerns the environment for internal and external risk management communication, and the policies that reinforce risk management. Strategic risk management addresses managerial decision making – determining how management weighs risk in terms of likelihood, potential effects on credit, liability management and financing decisions. In April of 2010 S&P discussed its approach to the review of nonfinancial companies at the Risk and Insurance Management Society Conference. They indicated that they are looking for:

- An approach to attend to key risks
- Conscious risk selection
- Awareness of risk tolerance/appetite
- Knowledge of what can go wrong
- Having a “Plan B” for risk responses
- Avoidance of outsized risks
- Resilience to risk events

The other rating agencies are following suit with evaluation plans of their own, with A.M. Best having taken a strong position on its use of ERM for the insurance industry.

ERM and Corporate Governance

The NYSE requirements that Audit Committees discuss the company's guidelines and policies regarding risk assessment and risk management, and the SEC disclosure rules that went into effect February 28, 2010 requiring companies to discuss the role of the board in overseeing risk management have certainly

heightened the awareness of board members in overall risk management responsibilities and the potential use of ERM. The SEC rules provide that companies should consider having individuals who supervise the day-to-day risk management responsibilities report directly to the board or to a board committee. Also, Delaware law now specifies that directors have a duty of oversight that requires them to implement and oversee the operation of reasonable information and reporting systems or controls designed to inform them of material risks.

Clearly, risk governance has become an important component of corporate governance. The National Association of Corporate Directors formed a blue ribbon commission that submitted a report in 2009 outlining the risk oversight responsibilities of board members and developed the following ten principals to guide directors in their efforts to provide effective oversight of risk:

1. Understand the company's key drivers of success.
2. Assess the risk in the company's strategy.
3. Define the role of the full board and its standing committees with regard to risk oversight.
4. Consider whether the company's risk management system – including people and processes – is appropriate and has sufficient resources.
5. Work with management to understand and agree on the types (and format) of risk information the board requires.
6. Encourage a dynamic and constructive risk dialogue between management and the board, including a willingness to challenge assumptions.
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 board's risk oversight processes: do they enable the board to achieve its risk oversight objectives?

The Current State of ERM Implementation

Even with the growing pressure for more effective risk oversight from regulatory bodies and rating agencies, recent surveys show that the level of enterprise-wide risk oversight is still relatively immature. However, there are emerging trends that indicate that the development of risk management oversight from senior management and board levels is in place or growing in many organizations.

KPMG released enterprise risk management survey results in January 2009 that indicated that companies fall short in three areas of their enterprise risk management programs – risk culture, risk management processes, and technology. Participants in this survey were internal auditors and board members

of companies. As far as risk culture, 58% of the respondents indicated that their employees in general did not have an adequate understanding of how risk exposures should be assessed for likelihood or impact. Only 13% of internal auditors surveyed have consolidated risk assessment procedures, and only 25% of the internal auditors indicated that their companies apply technology to their ERM programs although another 25% were considering it.

In February 2010, North Carolina State University, which has a significant educational program in enterprise risk management, *The ERM Initiative*, released a survey report in which 331 business entities participated. The key findings of the survey included:

- Over 63% of respondents believe that the volume and complexity of risks have changed “Extensively” or “A Great Deal” in the last five years.
- 39% of respondents admit they were caught off guard by an operational surprise “Extensively” or “A Great Deal” in the last five years. Another 35% noted that they had been “Moderately” affected by an operational surprise
- 49% of respondents describe the sophistication of their risk oversight processes as immature to minimally mature, and almost 57% of respondents have no formal enterprise-wide approach to risk oversight.
- Almost 57% of the respondents have no formal enterprise-wide approach to risk oversight and 48% 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.
- For almost half (45%) of the organizations represented, the board of directors is asking senior executives to increase their involvement in risk oversight.

The Risk & Insurance Management Society has released “RIMS State of ERM Report ” which has 564 organizations participating. A number of significant findings are included in the report, including the “verification from businesses that ERM boosts business performance.” The study found that 93% of organizations with formalized ERM programs in place make better risk-informed decisions.”

The RIMS Technology Advisory Council has also compiled a recent report on ERM technology solutions, recognizing that technology solutions can provide strong support for the ERM process. A survey of various size companies across various industry groups was part of the report, and the survey found that 51% of respondents had an ERM process in place, and of the respondents using ERM, 47% used a software support tool for implementation of ERM.

ERM and the Recent Financial Crisis

ERM has been mentioned regularly over the last year in connection with the continuing worldwide financial crisis. By late 2007 and early 2008 the blame for the crisis was being placed on poor risk management practices. In mid-2008 as the breadth of AIG's financial difficulties became apparent, Maurice "Hank" Greenberg, former Chairman and CEO of AIG, blamed the problems on the failure of internal risk management. He wrote the following statement for an October 2008 hearing by the House Committee on Oversight and Government Reform, "Reports indicate that the risk controls my team and I put in place were weakened or eliminated after my retirement."

The Risk and Insurance Management Society (RIMS) has taken the position that the financial crisis resulted from a system wide failure to embrace appropriate enterprise risk management behaviors, or attributes, within these distressed organizations. RIMS believes there was an apparent failure to develop and reward internal risk management competencies, and a failure to use enterprise risk management to assist management's decision making for both risk-taking and risk-avoidance decisions. Also, there was an over-reliance on financial models, with the mistaken assumption that the "risk quantifications" (used as predictions) based solely on financial modeling, were both reliable and sufficient tools to justify decisions to take risk in pursuit of profit.

Wortham's Role in the Process

As an independent firm Wortham is able to select among the "best in class" third party service providers when it comes to ancillary risk management services. This insures that our clients are provided with the best solutions to their risk management issues. For many years, Wortham has assisted clients with certain aspects of the ERM process – exposure analysis (through a proprietary exposure survey), risk frequency and severity analysis, risk mapping, and a risk information management system.

There are arrange of approaches, beyond that provided directly by Wortham, that can be used in developing an Enterprise Risk Management process – utilization of software solutions that provide assistance with in-house ERM plan development, to third party consultants – boutique ERM consultants or the ERM consulting practices at large audit forms or consulting practices. Our capability to provide introductions for clients to such service providers is a product of our independence and desire to furnish clients with a quality solution.