ERM in Strategic Planning

Companies engaged in ERM take what is considered a portfolio or enterprise-wide view of risk, addressing challenges in each area and, ideally, linking them to strategic planning. This is a departure from the silo-based approach many organizations took in the past, in which each operating function or division tackled risk independently. The risks addressed under ERM include not only potential changes in areas such as interest rates and broad economic indicators, but also in specific markets, countries, customers, vendors, suppliers, labor markets and technologies, as well as threats from natural and man-made disasters. The point is to examine the company’s entire range of assets – including human resources, intellectual property, customer relationships, suppliers, facilities and more – in identifying and addressing risk.

Audit committees were also given wider responsibilities under SOX, and the rules of the major stock exchanges followed suit. For example, the New York Stock Exchange Corporate Governance Rules require that listed companies’ audit committees have written charters stipulating the committee’s responsibilities, including the duty to discuss risk assessment and risk management policies. The SEC requires issuers to report certain risk factors in Item 1A, “Risk Factors,” in Form 10-K. Companies also must give the SEC quarterly updates on changes affecting these factors.

The point is to examine the company’s entire range of assets – including human resources, intellectual property, customer relationships, suppliers, facilities and more – in identifying and addressing risk.

Important Frameworks

Beyond regulatory requirements, other valuable tools are available to companies to help them address regulatory compliance issues and a range of other needs. For example, in 2004 the spotlight on ERM was enhanced when the Committee of Sponsoring Organizations (COSO) of the National Commission on Fraudulent Financial Reporting (also known as the Treadway Commission)
published *Enterprise Risk Management – Integrated Framework*. The COSO framework consists of eight interrelated components:

- Internal environment
- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Other key frameworks of value to companies are COSO’s *Internal Control – Integrated Framework*; and *Enterprise Governance: Getting the Balance Right*, from the International Federation of Accountants (IFAC).

The IFAC study said an efficient and effective risk management framework should give the board greater confidence in the organization’s risk management capability; allow the board to challenge management; and reassure shareholders about the organization’s commitment to risk management. Not surprisingly, highly regulated banking and financial services organizations tend to have the most developed ERM processes.

**How Are Public Companies Applying ERM?**

Many board and management responsibilities already encompass risk considerations, especially in light of changes organizations have made to comply with SOX. While many organizations generally are on the threshold of adopting ERM, wide implementation on a truly enterprise-wide basis has yet to occur. One factor, experts note, is that in recent years, companies have been so preoccupied with understanding and complying with SOX that they have lacked the time or resources to focus on other initiatives that might add overall value but do not specifically meet any current compliance requirements.

The PricewaterhouseCoopers 7th Annual Global CEO Survey, *Managing Risk: An Assessment of CEO Preparedness*, found a large gap between the adoption of the basic processes of ERM and the level of full implementation in all respects. The survey found that about two-thirds of the surveyed companies have basic processes in place, while one-third of the companies have achieved full implementation. One factor behind the gap is the degree of commitment to ERM at the CEO and board levels, as well as within the company as a whole, the survey said.

Even organizations that believe they are addressing risk issues may not be adequately doing so, according to an analysis by the Conference Board in conjunction with McKinsey & Co. and KPMG’s Audit Committee Institute (*The Role of the U.S. Corporate Board of Directors in Enterprise Risk Management*). While companies tackle problems as they arise, “they may not have adequately robust and systematic enterprise risk management processes in place,” Conference Board officials said.

Corporate directors appear to be more optimistic than they were in the past regarding companies’ approaches to risk. In a June 2006 Conference Board study, 10.5% of directors did not think they had a comprehensive understanding of the risks facing their companies, down from 36% in a similar 2002 study. At the same time, directors who serve on more than one board said there was little consistency in the approach to risk and that few had firmly established risk procedures.

The survey found that about two-thirds of the surveyed companies have basic processes in place, while one-third of the companies have achieved full implementation.

Although the COSO ERM framework has its critics, those with extensive corporate experience assert that it offers a simplified structure that can be adapted for various uses. The framework is considered by many to be a very effective way to organize information. When implementing the framework, some companies have taken a checklist approach, in which the company essentially runs through the framework’s elements and conducts an inventory that considers its own efforts in each category.

**Assigning Responsibility**

It is not yet clear where responsibility for ERM will rest. In a 2005–2006 KPMG Audit Committee Institute survey, more than half of audit committee members believed the audit committee should not have the main responsibility for the organization’s entire risk management program. Many
reported the process for assigning risk oversight responsibilities was not well defined in their organizations.

According to the Conference Board study, at about two-thirds of Fortune 100 companies, responsibility for board risk rests with the audit committee; another committee shares the responsibility with the audit committee in 23% of companies. While the audit committee might be the top choice for risk management oversight responsibility, Caryn P. Bocchino of KPMG’s Audit Committee Institute, who worked with the Conference Board on its study, noted that, given audit committees’ existing responsibilities, boards might consider assigning nonfinancial reporting aspects of risk management to another body that would work with the audit committee.

Some companies have created a chief risk officer (CRO) position responsible for evaluating risks and devising approaches to address them. The CRO might report to the head of internal audit or to the CFO, depending in large part, experts note, on how much clout the CRO might realistically have under each function. However, the CRO position certainly has not yet become widespread, because organizations still struggle with turf issues and other logistical questions. In financial organizations – the industry that is considered most advanced in its ERM efforts – 16.1% had a CRO who reported on risks to the board, up from almost none a few years ago, according to the Conference Board. At 71% of companies, this responsibility rested with the CFO.

As the ERM process evolves, the distinction between process and content is critical to the discussion. As discussed further below, a recommended practice is to give one group or position responsibility for creating risk strategy, while one or more other areas are charged with implementing these strategies throughout the organization and within various departments.

**Developing or Recommended Practices**

What ERM practices are in place or recommended? According to the PricewaterhouseCoopers survey, CEOs believe that full implementation of ERM is possible when:

- The CEO has the necessary information to manage risk at the enterprise level
- There is “a common terminology or set of standards” for managing risk
- ERM is fully included in the strategic planning process
- Risk management data are quantified as much as possible
- Risk management is fully integrated across all functions and business units
- All employees are aware of their level of personal accountability within the ERM framework
- The costs of regulatory compliance are closely monitored
- Regulatory compliance is closely managed to prevent noncompliance

What is a practical approach for implementing ERM across all functions? One practice at some companies is to create a cross-disciplinary internal risk management team made up of key representatives from various areas who might meet regularly to assess risks in and across their departments. In addition to proactive risk evaluations, the CRO might also implement a crisis management plan that would deal with natural disasters, product failures and tampering, terrorist attacks and similar threats.

Experts suggest that there are two facets to be considered as part of the overall process: identification of current risks; and targeting and management of ongoing and emerging threats.

Experts suggest that there are two facets to be considered as part of the overall process: identification of current risks; and targeting and management of ongoing and emerging threats. Management might be in a better position to identify existing risks while the board or a committee of the board might take over the ongoing analysis of new threats. A further step would be to align board committees with identified risk areas, with the audit committee taking responsibility for financial risks; an ethics or compliance committee addressing threats in those areas; an operations committee overseeing those risks; and the full board responsible for overall strategy.

Many companies begin the process with a simple test in one location or
function, in which new approaches are tested in an exercise that can be run by the CRO or chief audit executive. In addition, the internal audit team might take charge of an education effort to raise awareness throughout the organization and gather further information about the key risks identified within the different divisions.

Experts report that companies have the best success if they recognize that they already have in place many methods to identify, evaluate, respond to and mitigate risk – the very foundations for ERM. Businesses that are performing internal control assessments to comply with SOX have probably satisfied several of the COSO ERM framework elements. Many organizations find that the most challenging aspect of applying the COSO framework may be some of the subjective assessments it calls for, such as evaluating a company’s risk appetite.

**Experts report that companies have the best success if they recognize that they already have in place many methods to identify, evaluate, respond to and mitigate risk – the very foundations for ERM.**

Within COSO’s *Internal Control – Integrated Framework*, the definition of internal control extends beyond financial reporting compliance to operations and compliance objectives. Although this document’s discussion of the role of the audit committee is focused on financial reporting, it has been considered good practice for internal audit departments to have a dotted-line reporting relationship to the audit committee, and to have internal auditing standards encompass the broad definition of internal controls.

Internal audit standards with respect to ERM provide some direction as well. These standards charge internal audit with responsibility for evaluating the effectiveness of the organization’s risk management system, including design and function of processes; effectiveness and efficiency of risk responses and control activities; and completeness and accuracy of risk management reporting.

Both management and the audit committee should be involved in internal control and risk management processes as they relate to nonfinancial reporting objectives. One foundation for this assertion is the audit committee’s responsibility for the external audit relationship and external auditing standards under both the PCAOB’s Auditing Standard No. 5.

**Implementing Change**

ERM has clearly been established as an important goal for all public companies and their audit committees. While the role of the audit committee is not yet sharply defined, it will certainly be a significant one. Moving forward, committees will undoubtedly be expanding their understanding and involvement in this area.

**Executive Summary**

» Several studies suggest that management and audit committees must play meaningful roles in implementing a more comprehensive approach to enterprise risk management (ERM).

» The New York Stock Exchange Corporate Governance Rules require that listed companies’ audit committees have written charters stipulating the committee’s responsibilities, including the duty to discuss risk assessment and risk management policies and CFOs of public companies on the effectiveness of internal controls over the company’s financial reporting and gave audit committees wider responsibilities.

» PricewaterhouseCoopers’ 7th Annual Global CEO Survey found that about two-thirds of the surveyed companies have basic ERM processes in place, while one-third of the companies have achieved full implementation.


» Companies have the best success if they recognize that they already have in place methods to identify, evaluate, respond to and mitigate risk – the very foundations for ERM. Businesses that are performing internal control assessments to comply with SOX have probably satisfied several of the COSO ERM framework elements.
QUESTIONS FOR AUDIT COMMITTEE MEMBERS TO ASK

• What is the audit committee’s role in enterprise risk management for the company?
• What should be included in the audit committee’s charter on responsibilities for enterprise risk management?
• What process should be used to inform the Board of Directors of specific risk areas?

Anita Dennis is a freelance business writer and regular contributor to the JofA. The author thanks Dennis Chookaszian, Patricia Cochran, John Farrell and William G. Shenkir for their contributions to this article.

AICPA RESOURCES
Audit Committee Effectiveness Center
https://www.aicpa.org/audcommctr/homepage.htm

JofA articles
- “Eight Habits of Highly Effective Audit Committees,” Sept. 07, page 46
- “Internal Control Guidance: Not Just a Small Matter,” March 07, page 46
- “A Changing Corporate Culture,” March 04, page 57
- “Beyond Traditional Audit Techniques,” July 02, page 28

Publications
- The AICPA Audit Committee Toolkit(s) (#991001, #991004, #991005)
- COSO Enterprise Risk Management – Integrated Framework (#990015)
- Identifying, Measuring, and Managing Organizational Risks for Improved Performance (#030001PDF, download)
- Risk Assessment Suite of Standards (#060704)

CPE
Internal Control Essentials for Financial Managers, Accountants and Auditors, a CPE self-study course (#731853)
(For more information, or to register or make a purchase, go to www.cpa2biz.com or call the Institute at 888-777-7077.)

OTHER RESOURCES
Regulations

Surveys and Analyses
- Internal Controls – A Review of Current Developments, www.ifac.org

- Enterprise Governance: Getting the Balance Right, www.ifac.org
- NC State ERM Initiative http://mgt.ncsu.edu/erm/

DISCLAIMER: This publication has not been approved, disapproved or otherwise acted upon by any senior technical committees of, and does not represent an official position of, the American Institute of Certified Public Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this publication. If legal advice or other expert assistance is required, the services of a competent professional should be sought.