Audit Committee Involvement in Risk Management Oversight

Embracing emerging expectations for risk management leadership.

December 21, 2007
By Mark S. Beasley, Deloitte Professor of Enterprise Risk Management

The volume and complexity of risks facing enterprises across most industries are at all time highs. Combined with that is a continued increase in expectations that boards of directors and senior executives are effectively managing the portfolio of risks for the enterprise. To respond to these challenges, many boards of directors are directing executive management of organizations to embrace enterprise risk management (ERM) to develop a stronger top-down holistic view of enterprise-wide risks. In most cases the board is delegating oversight of management's risk processes to an already challenged audit committee.

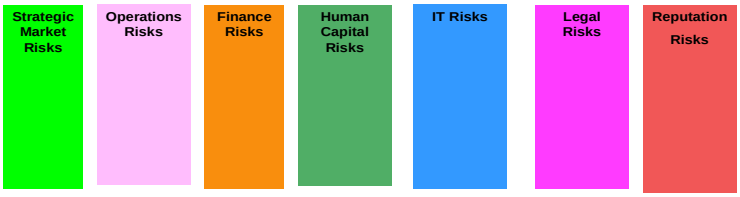
Drivers of Risks

Most argue that the profile of risks affecting enterprises today is vastly different than risks impacting enterprises a decade ago. Changes in technology, globalization, the nature of business transactions, such as derivatives and hedging, and the rapid evolution of business life cycles create tremendous challenges for boards and senior executives as they attempt to manage risks that might derail an enterprise's ability to accomplish critical objectives. Risk drivers, such as the recent sub-prime lending meltdown, can arise from both internal and external events and quickly impact an enterprise in significant ways overnight. As a result, the challenge facing audit committees and boards to effectively oversee numerous complex risk drivers can be daunting.

Enterprise Risk Management

To meet these challenges, many boards and senior executives are changing the way they think about managing risks throughout their business. While businesses have managed risks for centuries, the traditional approach to risk management has been to assign risk oversight responsibilities to certain business functions, such as legal or IT, where risks are managed in isolation by that function. Such an approach is often described as a "silo" or "stove pipe" approach to risk management, as illustrated in Figure 1 by the stand alone silos of functional areas. Unfortunately that traditional approach fails to recognize the reality that individual categories or "silos" of risks often interact with other silos. As a result, one function may be lobbing risks unknowingly to other functions within the same organization, which often results in either no reduction in risk or even increases in risks for the enterprise as a whole. Furthermore, traditional risk management approaches often fail to develop a common way of thinking about "risks," which leaves the interpretation of what constitutes a risk and what level of risk is acceptable to each silo leader. And for some, the approach to risk management is left to ad hoc, gut-level knowledge and management of key categories of known risks.

Traditional Risk Mgt Approach



"Silo" or "Stove-Pipe" Risk Management

Figure 1

Leading best practices now call for boards and senior executives to move from an ad hoc approach to risk management to one that leads to a more structured enterprise-wide view of risks affecting the enterprise. This new approach, known as enterprise risk management (or "ERM"), represents a change in the way of thinking about risks for the organization. While retaining the need for risks to be managed and owned at the business function level, the embrace of ERM involves a shift in processes and culture by strengthening communication, training, and awareness, and building processes to track risks so that individual risk silo managers begin to view risks through an enterprise lens and help build an enterprise-wide analysis of risks for senior executive and board review.

Several conceptual frameworks have been developed to assist boards and senior executives in leading the implementation of ERM. In 2004, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued its *Enterprise Risk Management – Integrated Framework* with this definition of ERM:

> *Enterprise risk management is a process, effected by the 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 risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of objectives.*[1]

This definition emphasizes several key concepts. First, ERM must be driven from the top of the organization, including involvement by the board. Second, ERM is meant to be value-adding, and thus risk analyses should be integrated with strategy planning. Third, the goal of ERM is not risk reduction. Rather, ERM is designed to increase the likelihood that risks are effectively managed by creating an enterprise-wide view of risks

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, September 2004, www.coso.org, New York, NY.

so that organizational objectives are more likely to be achieved for value preservation and enhancement as illustrated by Figure 2.

Figure 2

Role of the Board and Audit Committees

The board of directors and its audit committee play a critical role in ERM by establishing the right environment or tone at the top for the embrace of ERM by senior executives and others throughout the enterprise. Given the board's responsibilities for representing the interests of shareholders, the board plays a vital role in overseeing management's approach to ERM, including the determination of the enterprise's appetite for risks. Without board oversight, ERM may not be embraced by senior management or risks may be managed to be within management's tolerances for risks, which may differ from those of key stakeholders.

External drivers are encouraging boards to oversee management's ERM practices by assigning explicit responsibilities to audit committees for risk oversight. The New York Stock Exchange's (NYSE) Final Corporate Governance Rules require audit committees to discuss policies with respect to risk assessment and risk management. While acknowledging that an entity's senior executive team has the job of assessing and managing the entity's exposure to risk, the NYSE rules call for the audit committee to discuss guidelines and policies to govern the process by which this is accomplished and to discuss the entity's major financial risk exposures. Standard & Poor's recently announced plans to expand its evaluation of an enterprise's ERM processes as part of their debt rating analysis and scoring.[2] A key element of S&P's ERM evaluation focuses on the entity's risk management culture and governance, which includes an analysis of the board and audit committee's role in risk oversight. Similar considerations are

[2] Standard & Poor's, Criteria: Request for Comment: Enterprise Risk Management Analysis for Credit Ratings of Nonfinancial Companies, November 2007, www.standardandpoors.com, New York, NY.

performed by Moody's and Fitch as well. Thus, the board and audit committee's involvement in ERM oversight is becoming a critical component of effective governance.

Developing Audit Committee Processes

Despite the incredible demands now placed on audit committees, those who serve on these committees are examining how their processes need to be enhanced to meet these increasing expectations for audit committee oversight of risk management activities. They are seeking best practices and training to help them identify their role in overseeing management's risk procedures, including their review and approval of key risk policies, risk authorities, and risk tolerances. Audit committees are exploring methods for evaluating management's infrastructure, including personnel competencies and technologies and communications, to ensure that risk information they receive is providing the appropriate top-down, enterprise view of risks.

As audit committee involvement in ERM oversight evolves, more of those who serve are beginning to realize the benefits of better risk intelligence for them in their governance roles. Many are learning that ERM is producing better risk insights that help the board in its strategic oversight by identifying events that might create risk opportunities as well as risk threats to accomplishing strategic objectives. In addition, better risk intelligence means audit committees and the full board can be better informed about areas requiring greater governance oversight as well. So, in the end, the increase in audit committee and board risk management oversight is strengthening the board's ability to protect and enhance stakeholder value.

Dr. Mark Beasley, is the Deloitte Professor of Enterprise Risk Management and Director of the ERM Initiative in the College of Management at North Carolina State University in Raleigh, NC. The ERM Initiative provides thought leadership on enterprise risk management, with an emphasis on the role of ERM in strategy and governance (see www.erm.ncsu.edu). Dr. Beasley serves on the COSO Board representing the American Accounting Association, and he is a frequent speaker on ERM and governance at national and international conferences.

The AICPA and NC State's ERM Initiative are jointly hosting a one and a half day workshop titled, ***The Audit Committee's Role in Risk Oversight: Taking a Strategic View of the Enterprise***, to help audit committee members understand emerging expectations for greater risk oversight. This workshop will be conducted at the AICPA's New York City offices on October 23-24, 2008.