

# Enterprise Risk Management: Who's in Charge?

By Rick W. Julien and Jonathan T. Marks

## ERM governance roles and responsibilities.



Rick W. Julien



Jonathan T. Marks

In response to recent events that have affected many markets—as well as competitive pressures, regulatory scrutiny, and other factors—more and more publicly traded corporations are reviewing their approach to enterprise risk management (ERM). Board members are asking questions about

the organization's risks and the ERM process itself—and many are expressing concerns.

The most frequently cited concerns involve the fundamental questions of just what ERM is and who is responsible for ensuring that the process is effective and sustainable: Should the full board be involved in risk discussions, or should it appoint a designated committee to oversee ERM development and execution? What is the role of the audit committee? What about the internal audit group and the leaders of various business units?

All of these individuals and groups have legitimate—but widely varying—roles in risk management. Under a typical ERM scenario, all of them share ownership or oversight of risk and must help the organization identify,

manage, and quantify risks. So how do these disparate players balance their specific interests and obligations? And who is responsible for the broader strategic risks and the process itself?

### Why ERM governance is a challenge

This ambiguity about ERM roles and responsibilities might seem disconcerting at first, but it really should be expected. After all, ERM is still an evolving process in many organizations.

Moreover, in most companies a variety of risks are already being managed in diverse ways, with varying degrees of success. While these non-integrated risk management activities might have been effective in their limited scope, there are often no clear links to broader business strategies. Establishing these links—and defining the system for overseeing them—can cause confusion in terms of roles and responsibilities.

The complexity and comprehensive nature of ERM also add to the governance challenge. The integrated ERM model introduced in 2004 by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission organizes risk into four general groups: strategic, operational, reporting, and compliance. Each of these is then defined along a scale that addresses eight stages of ERM maturity. The resulting matrix, which has been compared to a Rubik's Cube®, is often too complex for many organizations' needs.

### Identifying the key players

In general terms, the CEO is responsible for reporting risk to the board, and the board as a whole is responsible for assisting the CEO with risk oversight, especially as it relates to the principal risks affecting the corporate strategy. But this broad understanding leaves many questions unanswered when it comes to the specifics of launching and executing a successful ERM approach.

One absolutely critical requirement is strong support from the CEO. This must be reinforced by support from other key executives, who invest their commitment in a chief risk officer or ERM leader who is recognized and respected. Above all, the ERM process should be linked to other management activities, especially strategic planning and budgeting. This integration of risk management activities into the organization's processes is one of the hallmarks of ERM maturity.

One such integration opportunity is to link the ERM activities into the overall good governance processes of the board and the organization.

In an attempt to link the two, we need to define governance roles with greater precision, to differentiate clearly between the company activities and the board responsibilities. In some organizations, the ERM oversight responsibility is assigned to the audit committee, while in still others this responsibility is taken on by the entire board or not addressed at all. One emerging practice is establishing a

board risk committee, which is given specific responsibility in assist the board of directors in fulfilling its risk oversight responsibilities, including overseeing ERM implementation and execution.

In addition, several possible approaches can be taken to define the relationship between these board committees and the internal risk management and audit functions. This variety of approaches sometimes creates confusion for those who are attempting to implement an ERM process.

## **An ERM governance model**

Most ERM initiatives begin as a project for someone within finance or internal audit, who typically is charged with launching an initial pilot effort. As the ERM process matures, a broader and more integrated governance and management structure must evolve.

Eventually, the structure that develops will be specific to each organization. What follows is one general approach, which should be regarded as a series of guidelines rather than a specific prescription. Companies still in the early stages of their ERM journey may find it a useful road map. Those who are further along should look at it as a template to be tailored to reflect each individual organization's unique structure and challenges.

This successful ERM governance model centers on two internal groups, which for purposes of discussion we have designated the Risk Management Council and the ERM Leadership Team.

## **Risk Management Council**

Charged with providing executive ERM leadership, the Risk Management Council reports to the CEO. Its members might include

the corporate general counsel, chief audit executive, and other senior level executives, as well as the top executives of major business units. In addition to overseeing and monitoring the ERM strategy and infrastructure, this council defines the appetite and tolerance for risk, which ultimately must gain board approval. It also monitors the reporting of significant risks and responses, ensures the overall corporate strategy is risk-responsive, and provides direction and oversight to the chief risk officer and ERM Leadership Team.

## **ERM Leadership Team**

Led by the chief risk officer or someone else who understands risk management, this team oversees the actual execution of ERM-

related activities. It also develops risk management awareness, and implements the appropriate ERM infrastructure. This infrastructure includes a common risk model and definitions, a consistent method of risk assessment, and risk documentation procedures and standards. The team's membership may include some members of the Risk Management Council, such as the general counsel and chief audit executive, as well as compliance risk officers and representatives from individual business units.

These two internal groups maintain a somewhat complex relationship with the board of directors. For example, the ERM Leadership Team reports to the internal Risk Management Council, but the team's chair may

also provide reports to the board's audit committee or designated risk oversight committee. This board committee reviews, monitors, and reports to the full board on the effectiveness of the organization's various risk-oriented groups.

While the particulars of this governance structure will vary from company to company, one critical factor is the linkage between the ERM process and the ownership and oversight of risks. Additionally, the organization must link the ERM process to other key management functions, including strategy, budgeting, compliance, audit, environmental, and new business development. These links help gain support and reduce potential resistance to fully adopting ERM, and also

*In general terms, the CEO is responsible for reporting risk to the board, and the board as a whole is responsible for assisting the CEO with risk oversight.*

increase the effectiveness of the effort and facilitate knowledge sharing.

By identifying and managing the risks that can keep an organization from achieving its business objectives, the risk management governance structure helps the organization achieve the full benefits of ERM—with less internal confusion. These benefits may include improved operational performance, enhanced corporate governance, reduced compliance costs, and, above all, increased shareholder value.

---

Rick Julien is an executive with Crowe Horwath LLP in the Oak Brook, Ill., office. He can be reached at 630.586.5280 or rick.julien@crowehorwath.com.

Jonathan Marks is an executive with Crowe Horwath LLP in the New York office. He can be reached at 212.692.3727 or jonathan.marks@crowehorwath.com.