Chapter 14

Appendix C: Enterprise Risk Management: Ask the Board

The recent wave of business scandals and threatening world events has fostered a greater awareness of the importance of risk management as a component of corporate governance. In 2004, the so-called Committee of Sponsoring Organizations of the Treadway Commission (COSO) released a comprehensive report titled "Enterprise Risk Management—Integrated Framework" to provide companies with a roadmap for identifying risks, avoiding pitfalls, and taking advantage of opportunities to grow firm value.

COSO defines enterprise risk management (ERM) as

a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.PricewaterhouseCoopers (2004). Principles-Based Framework for Managements and Boards to Comprehensively Manage Risks to Objectives (released by COSO, available at http://www.coso.org).

So defined, ERM assists in

- *aligning risk appetite and strategy* by explicitly considering the organization's risk appetite in evaluating strategic alternatives, setting related objectives, and developing mechanisms to manage related risks;
- *enhancing risk response decisions* by providing rigor to identifying and selecting among alternative risk responses—risk avoidance, reduction, sharing, and acceptance;
- *reducing operational surprises and losses* by enhancing the capability to identify potential events and establish responses, thereby reducing surprises and associated costs or losses;
- *identifying and managing multiple and cross-enterprise risks* by facilitating integrated responses to multiple risks across the organization;
- *seizing opportunities* by considering a full range of potential events, which allows management to identify and proactively realize opportunities;

- *improving deployment of capital* by obtaining robust risk information, which allows management to effectively assess overall capital needs and enhance capital allocation.

Whereas traditional risk-management approaches are focused on protecting tangible assets shown on a company's balance sheet and related contractual rights and obligations, the scope and application of ERM are much broader. ERM's focus is *enterprise-wide*, and on *enhancing as well as protecting the tangible and intangible assets* that define a company's business model. This widening of the scope of risk management reflects the fact that—with market capitalizations often significantly higher than historical balance-sheet values—the extension of risk management to intangible assets is critical. Just as future events can affect the value of tangible physical and financial assets, they can also affect the value of key intangible assets, such as a company's reputation with suppliers, innovation record, or its brands.

ERM explicitly recognizes that risk may originate inside or outside the organization. For example, *environmental* risk originates outside the organization and can impair the viability of a particular business model. *Process* risk factors tend to be internal in origin and affect the ability of the firm to execute its stated mission. *Information for decision-making* risk threatens value creation because of its impact on the timeliness, quality, reliability, and comprehensiveness the information used to make key decisions.

Because risks do not always fall clearly into one category, the ERM philosophy encourages companies to develop a comprehensive risk-management plan in which the approaches to the various components of risk interact with and influence one another. In particular, ERM looks at eight sets of issues:

- *Internal environment*. The tone of an organization is set at the top of the organization. It is, therefore, important to ask what appetite its leaders have for risk and whether the company's culture supports the chosen risk profile and risk-management and internal controls process.
- *Objective setting*. Companies typically set goals on many levels: strategic, operating, and financial. By clearly identifying its goals, management and the board can more clearly perceive the risks that the company may encounter.
- *Event identification*. The board should ask management how the company identifies new risks and opportunities. What risks and trends exist in the company's industry? What risks are associated with new products, services, or acquisitions? With new competitors? How are the company's risks interrelated? The board should also consider legal, ethical, and compliance risks that the company may encounter.

- *Risk assessment*. After identifying potential risks, management and the board should analyze and prioritize the risks in light of their likelihood and potential impact. Each business unit should be involved in the process and ask questions, such as, What adverse events has the company encountered in the past, and what lessons were learned?
- *Risk response*. Companies may chose to respond to risks by avoiding them or by accepting them and working to reduce their impact or dilute their severity by sharing risk with other parties. This raises questions, such as, What are the costs of these alternatives? Has management allocated sufficient resources to respond appropriately? Is the company adequately insured for its insurable risks?
- *Control activities*. The board should work with management to develop and implement well-structured policies and procedures in response to the company's primary risks to ensure that responsive actions are carried out at all levels of the company.
- *Information and communication*. Relevant information should be well documented and communicated on a timely basis—vertically, up and down the chain of management, and horizontally, across divisions of a company—to ensure that all members of the organization carry out their responsibilities with respect to the company's risk-management policies.
- *Monitoring*. The board should help management establish testing and evaluation procedures to monitor the company's risk-management system. Modifications to the risk-management system should be made as needed in response to these evaluations.

Although the management of a company is ultimately responsible for a company's risk management, the board must understand the risks facing the company and oversee the risk-management process. Board committees should incorporate risk management into their regular responsibilities. A company's governance committee can ensure that the company is prepared to deal with risks and crises by evaluating the individual capabilities of the directors, nominating directors with crisis-management experience, and considering the time each director and nominee has to devote to the company. The governance committee should also work with management to establish an orientation program for new directors and succession plans for key executive officers.

While some companies prefer to involve the board as a whole in the risk-management process, corporate governance guidelines and charters of audit committees may delegate this responsibility to the audit committee. Alternatively, a company may appoint a risk-management officer, form a risk-management committee, or assign responsibility to a finance or compliance committee of the board. The responsible committee or group should meet regularly with the

company's internal auditor, the chief financial officer, the general counsel, and the head of compliance and individual business units to discuss specific risks and assess the effectiveness of the company's risk-management systems.

Board committees should also incorporate risk management into their regular responsibilities. A company's governance committee can ensure that the company is prepared to deal with risks and crises by evaluating the individual capabilities of the directors, nominating directors with crisis management experience, and considering the time each director and nominee has to devote to the company. The governance committee should also work with management to establish an orientation program for new directors and succession plans for key executive officers.

14.1 Questions Boards Should Ask About Risk Management

The NYSE listing requirements specify that, when addressing the audit committee's duties and responsibilities, the committee charter should state that the committee must discuss management's policies with respect to risk assessment and management. The ERM framework provides a context for such a discussion. Examples of questions the committee should ask include

with respect to strategy,This appendix is from Waller, Lansden, Dortch, and Davis (2005).

1. Is the board effectively engaged in strategic discussion of the company's appetite for risk taking?
2. Does management involve the board when making decisions to accept or reject significant risks?
3. Is the company taking risks the board does not understand?
4. Are the risks inherent to the company's business model fully understood? Managed capably? Monitored in a timely fashion?

with respect to policy,

1. How does management reward growth and innovation without creating unacceptable exposure to risk? Are there defined boundaries and limits that clearly specify behaviors that are off-limits?
2. Is there a proper balance between entrepreneurial and control activities? Are the risks associated with opportunity seeking clearly understood and managed?

with respect to execution,

1. Does management understand the uncertainties inherent in its strategies for the business?
2. Are there assurances that risk controls function properly?
3. Does the company have effective contingency plans to respond in event of a crisis?
4. What system of "early warning" signals does the company have?
5. Are there effective processes in place for identifying, measuring, and evaluating risk-management capabilities?
6. Has a risk officer or risk-management team been appointed?

with respect to transparency,

1. Is there an effective process for reliable reporting on risks and risk-management performance?
2. Does the company have an organizational structure in place to support enterprise-wide risk management?