Management Accounting Quarterly
VOL.5 NO.2
Winter 2004

Aligning Corporate Governance with Enterprise Risk Management

BY PAUL J. SOBEL, CPA, AND KURT F. READING, PH.D., CMA, CPA

MELDING ENTERPRISE RISK MANAGEMENT WITH GOVERNANCE MEANS DIRECTORS, SENIOR MANAGEMENT, INTERNAL AND EXTERNAL AUDITORS, AND RISK OWNERS MUST WORK INTERDEPENDENTLY.

Corporate scandals and diminished confidence in financial reporting among investors and creditors have renewed corporate governance as a top-of-mind priority for boards of directors, management, auditors, and stakeholders. At the same time, the number of companies trying to manage risk across the entire enterprise is rising sharply. So, we ask, how can enterprise risk management (ERM) be integrated effectively with corporate governance?

RISK, ERM, AND GOVERNANCE

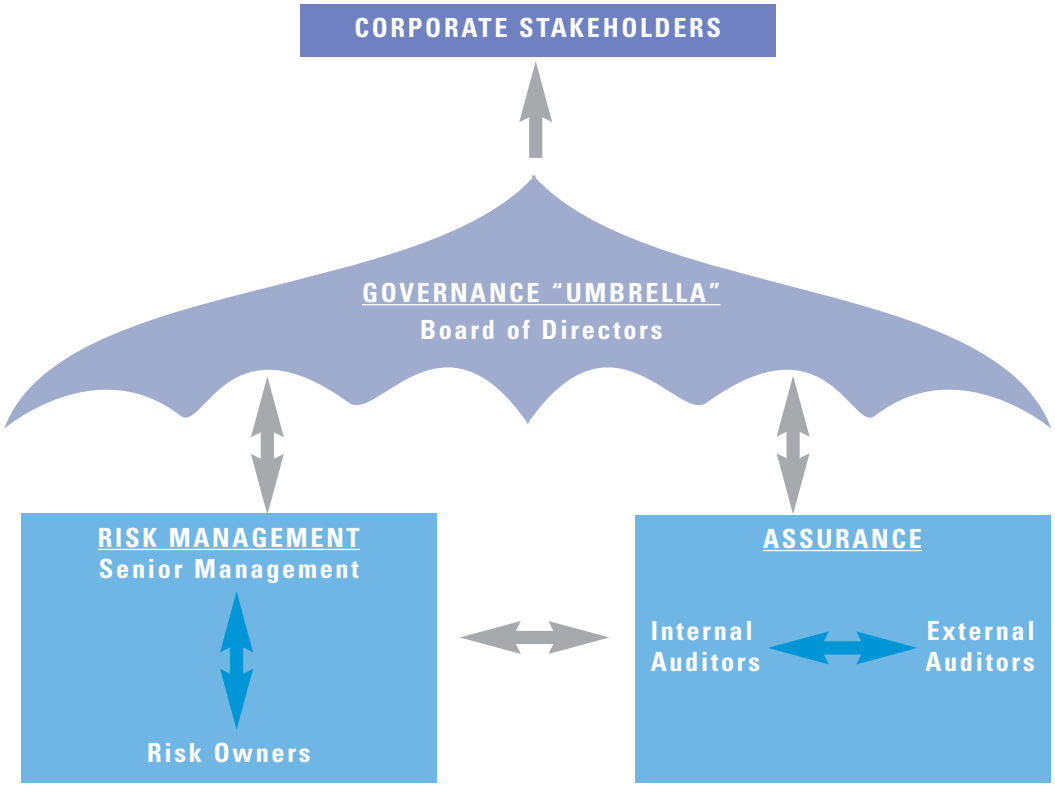
To begin, business risks, of course, are uncertainties that can impinge on a company's ability to achieve its objectives and can result in many interdependent outcomes—some negative, some positive. Moreover, risks are a function of severity and likelihood; they may or may not manifest themselves. If they do, a variety of exposures is possible.

Business risks relate to business objectives because risk taking is a prerequisite to success—without risk, there is no reward. Accordingly, some risks must be exploited to take advantage of strategic opportunities. Conversely, risks that threaten success must be mitigated. These risks include threats of problems occurring, such as misappropriation of assets, or opportunities not occurring, such as a failure to achieve strategic goals.

Meanwhile, ERM—a structured and disciplined approach to help management understand and manage uncertainties—encompasses all business risks using an integrated and holistic approach. A report from the Institute of Internal Auditors (IIA) captures the essence of ERM: "The goal of ERM is to create, protect, and enhance shareholder value by managing the uncertainties surrounding the achievement of the organization's objectives."[1] The professional literature indicates that ERM is relatively well understood, especially by the companies striving to implement it.

Finally, corporate governance is a process a board carries out to provide direction, authority, and oversight of management for the company's stakeholders.[2] Unfortunately, directors, management, internal and external auditors, and risk managers do not understand corporate governance well—especially from a day-to-day perspective. They sometimes consider it a nebulous topic: It "means different things to different

Figure 1: An ERM and Governance Framework



people."[3] Moreover, while the board of directors is the owner of the governance process, day-to-day guidance and oversight by the board clearly is not feasible; the board must rely on other parties—executives, managers, and auditors—to help it fulfill its governance responsibilities. But practical, how-to guidance for executives, managers, and auditors who are involved in corporate governance on a day-to-day basis is sparse.

An ERM and Governance Framework

Our ERM and governance framework, as illustrated in Figure 1, consists of four components: corporate stakeholders, the governance "umbrella" provided by the board of directors, risk management, and assurance. The arrows within and between the four components represent the various channels of ERM and corporate governance communications.

Who Should Be Responsible for What?

Boards of directors, senior management, internal auditors, and external auditors are "the cornerstones of the foundation on which effective corporate governance must be built," according to a position paper from the IIA.[4] Our conceptual framework also includes "risk owners." These are the people in a corporation who are responsible and accountable for managing specific risks, such as the chief legal officer, who is responsible for a company's legal risk. Only senior management and risk owners should be directly responsible for risk management. In Table 1 we delineate the primary risk management roles people in each group have as part of a company's governance.

Board of Directors. The board of directors is not directly responsible for risk management—that is management's job.[5] The board should, however, assume ultimate responsibility for corporate governance. The

Table 1: Who Should Be Responsible for What?

	RISK MANAGEMENT RESPONSIBILITIES?	PRIMARY ROLES IN CORPORATE GOVERNANCE
Board of Directors	NO	Provides risk management direction, authority, and oversight to senior management.
Senior Management	YES	Has primary responsibility for ERM. Delegates risk management authority, and specifies risk tolerance thresholds to risk owners. Reports ERM plans and performance results to the board of directors.
Risk Owners	YES	Assign specific risk management authority and risk tolerance thresholds to other personnel. Report ERM plans and performance results to senior management.
Internal and External Auditors	NO	Provide independent, objective assurance to senior management and the board of directors about the effectiveness of risk management, control, and governance processes.

board governs on behalf and for the benefit of the company's stakeholders, who include shareholders, employees, customers, suppliers, and others. The specific board committees to which corporate governance responsibilities are assigned vary among companies. For instance, two Unocal Corporation board committees concern themselves with ERM: the company's accounting and auditing committee and its corporate responsibility committee, according to an IIA report.[6] Further, a report from the Business Roundtable calls for a separate corporate governance committee to address governance issues and provide governance leadership.[7]

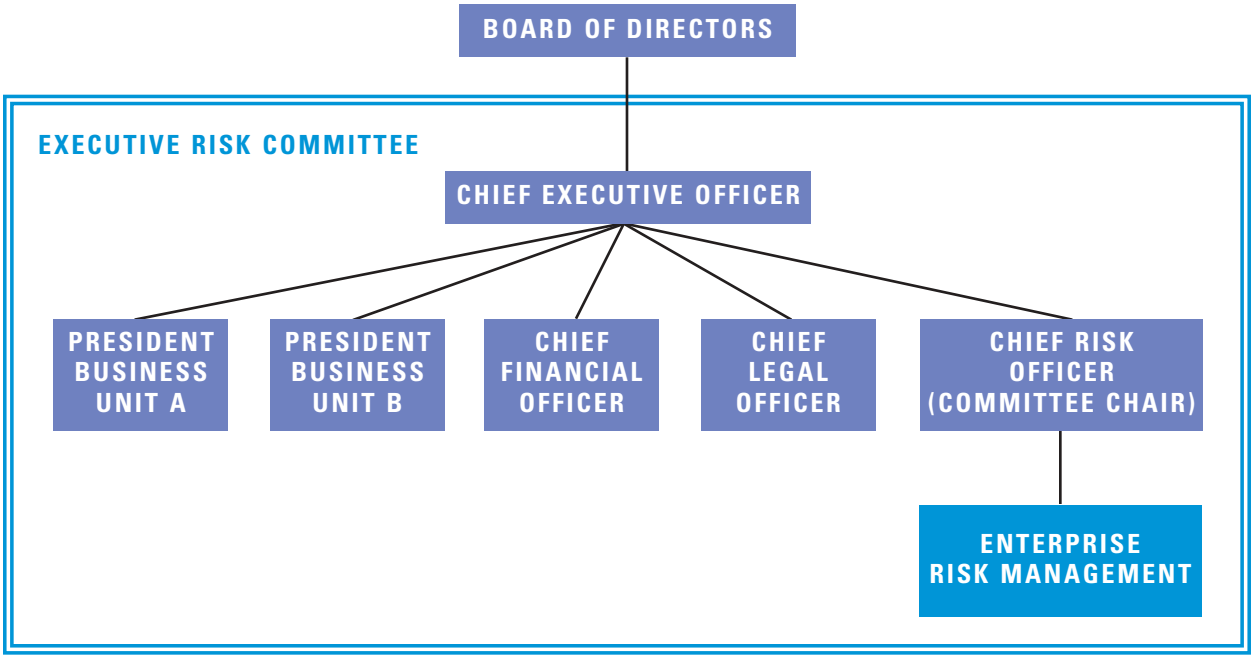
Although the board of directors should not assume direct responsibility for risk management, its governance activities contribute significantly to effective ERM, and boards must actively participate in risk management to add value.[8] The board should involve itself in the ERM process by providing direction, authority, and oversight to management. We offer directors the following suggestions:

- Contribute expertise, judgment, and professional skepticism to the strategic planning process;
- Define and communicate risk tolerance thresholds to senior management to guide management's decisions;
- Assign authority to senior management to manage risks within the specified tolerance levels;
- Oversee the implementation of the company's risk management process, and monitor the process to ensure that it continuously operates effectively in the best interests of the company's stakeholders; and
- Ensure that management's mix of performance indicators associated with key risks is aligned properly with the company's strategy and linked appropriately to shareholder value. The board should hold senior management accountable for keeping it apprised of significant risks, taking appropriate actions to manage these risks, and reporting risk management performance results.

The board should evaluate senior executives' performance and ensure that their performance targets and compensation are aligned with the company's strategy

Figure 2: Organizational Structure of an Executive Risk Committee

The chief risk officer (CRO), who oversees a company's enterprise risk management process, chairs the company's executive risk committee. Both the CRO and the chief executive officer are responsible for apprising the board of directors of key risk issues and initiatives.



and linked to shareholder value. It also should evaluate senior management's succession planning process to ensure that appropriately qualified people are ready to step in and carry on corporate executive duties when members of the senior management team turn over.

Management. In contrast to the board of directors, which "owns" the corporate governance process, management owns the ERM process.[9] Typically, senior management is responsible for designing and implementing a structured and disciplined approach to managing risks. Under senior management's supervision, risk owners develop, implement, perform, and monitor risk management capabilities and activities. Overall, risk management is most effective when (1) the chief executive officer is truly committed to the process, (2) other officers such as the chief financial officer and chief legal officer manage the risks under their jurisdiction, and (3) business unit executives and managers assume everyday responsibility for managing the risks under their control. Some companies have benefited greatly by having a chief risk officer (CRO) as the company's primary risk owner who oversees and coordinates the entire ERM process.

Senior management also plays an important role in corporate governance. Corporate executives who serve on their company's board of directors are perfectly positioned to facilitate the two-way communication that must occur between the board and the entire management team for effective governance to occur. An executive ERM committee can contribute to effective governance by directing and overseeing the ERM process on a day-to-day basis and monitoring a company's risk management decisions and activities. Four of the five companies studied in a 2001 report have formed one or more risk management committees or groups to oversee risk management activities.[10] Another company we studied—which, hereafter, we refer to as Company X because they wish to remain anonymous—has an executive risk committee that is chaired by the CRO and is composed of the chief executive officer and his or her direct reports, as shown in Figure 2. The executive risk committee delegates risk management

authority and specifies tolerance thresholds to risk owners who, in turn, assign more specific authority and tolerance thresholds to other personnel.

Internal and external auditors. Professional auditing standards, particularly those from the IIA and the American Institute of Certified Public Accountants (AICPA), preclude auditors from assuming management responsibilities such as making ERM decisions. Auditors may not, for example, dictate how key risks should be managed. They may, however, involve themselves in the ERM process by educating management about risk and controls, facilitating risk and control self-assessment sessions, serving on information system and other steering committees, recommending ERM process improvements, and performing other services of a consulting nature. (Such consulting-type services performed by auditors are excluded from the conceptual framework we discuss above and illustrate in Figure 1 because consulting is not an integral part of the corporate governance process.)

The role of auditors in the corporate governance process is to provide independent, objective assurance to senior management and the board of directors about the effectiveness of risk management, control, and governance processes. Such assurance may take different forms, as reflected in the following examples:

- When risk owners self-report upstream their assertions about ERM process performance, internal auditors may attest to the accuracy of the assertions.
- Internal auditors may directly evaluate ERM performance based on appropriate criteria and report their conclusions to senior management and the board of directors.
- Public accountants may uncover performance anomalies and/or control deficiencies during their examinations of a client's financial statements or during their examination of a client's internal control over financial reporting that must be reported to senior management and the board.

Who Should Communicate What to Whom?

The information that flows through the communication channels represented by the arrows in Figure 1 is critical to successful ERM and governance. Effective two-way communication must occur between: (1) the board and senior management, (2) senior management and risk owners, (3) management and auditors, (4) internal and external auditors, and (5) auditors and the board. Ultimately, the company is responsible to its stakeholders, and, accordingly, should communicate relevant risk management, control, and governance information to them.

Communications between the board and senior management. Ideally, ERM and governance responsibilities of the board and its committees are clearly articulated in charters and shared with senior management. That is the case, for instance, with Unocal Corporation, whose accounting and auditing committee's charter specifically refers to the committee's ERM responsibilities.[11]

Specific information relevant to both ERM and governance that the board of directors should communicate to senior management includes:

- The board's expectations of senior management for setting an appropriate tone for ethical behavior at the top of the company;
- The board's risk tolerance thresholds, together with authority to manage risks within the thresholds;
- Feedback to senior management about the mix of measures used to evaluate and monitor ERM performance; and
- The performance criteria and measures used by the board to evaluate executives' performance.

Senior management should report risk management plans and performance results to the board. In the case of United Grain Growers (now Agricore United) and Chase Manhattan (now JP Morgan Chase & Co.), the company has senior management committees that formally report risk management performance to designated board committees.[12] Company X, for instance, considers various risk and performance outcomes when making ERM performance and reporting decisions. This process evaluates potential outcomes and measures, board-level tolerance and reporting thresholds, and senior-management-level tolerance and reporting thresholds within six performance outcome categories: strategic, financial, legal and regulatory, reputation, people, and asset protection. It covers upside and downside, financial and nonfinancial, and leading and lagging performance indicators that are linked to shareholder value. In Table 2 we show one component of the com-

Table 2: Financial Outcomes and Measures of Enterprise Risk Mangement

CATEGORIES	POTENTIAL OUTCOMES	POTENTIAL MEASURES
◆ Financial	◆ Earnings, earnings before income taxes, earnings per share are below expectations	◆ Earnings per share, price/earnings ratio, other financial ratios
	◆ Negative cash flow/liquidity problems	◆ Liquidity ratios, cash forecasts
	◆ Credit rating downgrade	◆ Credit rating target
	◆ Inadequate/misleading disclosures	◆ Securities & Exchange Commission (or other) inquiries
	◆ Insufficient return on investment relative to allowable regulatory earnings	◆ Return on investment or return on assets ratios
	◆ Capital not available for growth	◆ Cost of capital
	◆ Capital misdeployed	◆ Return on invested capital ratio

munication process: the financial outcomes and measures that may impact governance decisions within a company.

Specific ERM and governance information that senior management should communicate to the board of directors includes:

- The steps senior management has taken to establish a healthy ethical culture and to handle significant code of conduct violations as they occur,
- Senior management's strategic objectives and its plan for achieving those objectives,
- The significant risks that affect the company's ability to achieve its strategic objectives,
- The actions management has taken or will take to manage those risks, and
- ERM performance results.

Communications between senior management and risk owners. Effective ERM and governance depend on clearly articulated corporate policy statements communicated downward by senior management. For example, FirstEnergy Corporation's risk management framework lays out the company's "constitution" for ERM.[13] The company's framework contains seven major sections: risk identification and definition, risk management, risk management practices, monitoring and reporting, communication and education, risk management philosophy, and risk management principles. DuPont's risk management framework includes three key components: a corporate-wide policy, corporate-wide guidelines, and line management strategies and procedures.[14]

Specific ERM and governance information that we believe senior management should communicate downward to risk owners includes:

- A written code of conduct that articulates the company's ethical principles and specific rules of conduct;
- A written risk management framework that conveys senior management's risk management philosophy, policies, strategies, and procedures; and
- Risk management authority, tolerance thresholds, and performance metrics for individual risk owners.

Relevant and reliable upward communication from risk owners to senior management is also imperative to effective ERM and governance. Company X's internal audit function assists risk owners in preparing the risk management plans they present to the executive risk committee. General Motors, for example, has managers report on the effectiveness of their risk management.[15]

We believe the specific information that risk owners

should communicate upward to senior management includes:

- Written assertions regarding compliance with the company's code of conduct,
- Risk and control assessments,
- Risk management plans, and
- ERM performance reports.

Communications between management and auditors. A clear understanding must be reached, preferably in writing, between auditors and management regarding specific assurance services to be provided. The IIA's Standards[16] call for internal auditors to formally define their purpose, authority, and responsibility in a charter that is approved by the board of directors. External auditors are encouraged by their professional standards to specify their contractual obligations to clients in engagement letters. Management must provide adequate information to the auditors for the auditors to complete their work.

Internal auditors' assurance reports include applicable conclusions and recommendations and may include action plans management agrees to. The conclusions, recommendations, and action plans are based on the auditors' evaluation of risk management performance. External auditors communicate to management any deficiencies in internal control over financial reporting uncovered during the course of their work. Whenever internal or external auditors uncover evidence that fraud may exist, they are required by their professional standards to bring the matter to the attention of an appropriate level of management.

Communications between internal and external auditors. Internal and external auditors should share information with each other and coordinate assurance activities to ensure proper coverage and minimal duplication of efforts. Such sharing of information may involve periodic meetings, reviewing each other's working papers and reports, and discussing relevant issues of mutual interest as they arise.

Communications between board members and auditors. The audit committee of the board of directors commonly oversees the work of internal and external auditors, calling on them to provide independent assurance about the company's risk management, control, and governance processes. It reviews the internal auditors' annual audit plan with the chief audit executive and the plans for auditing the company's financial statements and internal control over financial reporting with the external auditor.

Both internal and external auditors report significant outcomes of their work to the audit committee. Professional standards require auditors to report fraud and illegal acts involving senior management and significant control deficiencies to the audit committee. The IIA has called for internal auditors to report to the audit committee on the adequacy and effectiveness of internal controls,[17] just as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) reported in 1992.[18]

Communications to external corporate stakeholders. Because stakeholders are the primary "customers" of the governance process, a company's governance responsibilities are not fulfilled until pertinent governance-related information is reported externally.

Such public disclosures are increasing. Some companies, such as General Motors and Unocal Corporation, voluntarily publish corporate governance principles and guidelines. Stock exchanges in the U.K., Canada, and other countries require listed companies to disclose certain governance information. The Federal Deposit Insurance Corporation Act of 1991 requires large banks to issue management reports on the effectiveness of their controls over financial reporting and to obtain independent public accountants' opinions regarding management's assertions. The Sarbanes-Oxley Act of 2002 extends such requirements to all annual reports of publicly traded companies required by section 13(a) or 15(d) of the Securities Exchange Act of 1934.

Several organizations are putting pressure on companies to further expand and improve public disclosures of governance, risk management, and control information, among them the IIA and the National Association of Corporate Directors.[19]

Moreover, there have been recommendations that public companies issue reports covering risk management and all categories of controls, including financial, operational, and compliance.[20] The IIA suggests that such reports be based on information from several sources, including internal auditors' evaluations of risk

and control systems, evaluations of controls by financial statement auditors, management risk assessments and control effectiveness assertions, and the results of special investigations that could materially affect the board's decisions about risk management and control effectiveness.

COSO's New ERM Framework

In 2003, COSO issued an exposure draft of *Enterprise Risk Management Framework*, and the final draft is expected to be published in the summer of 2004.[21] This new framework outlines eight components of enterprise risk management, the following five of which most clearly support the ERM concepts we discuss above:

- **Internal environment.** This component encompasses the role that the board of directors plays in establishing a governance and risk management philosophy. Additionally, the concept of risk appetite is embedded in this component. Risk appetite is a key factor in our ERM and governance framework, as it is the foundation for establishing the risk tolerance direction provided by the board to senior management and by senior management to operating management.
- **Objective setting.** This component also makes reference to understanding and articulating a company's risk appetite when setting and communicating business objectives.
- **Risk response.** Embedded in this component is the notion that management may have different options for responding to risk. Management should communicate the option it chooses to the board to help directors carry out their governance oversight responsibilities.
- **Information and communication.** As we illustrate in Figure 1, multidirectional communications within the ERM and governance framework are the key bridges between different constituencies within the framework.
- **Monitoring.** The board of directors is responsible for monitoring how effectively management carries out governance that the board establishes. A company's monitoring must occur both at the activity or transaction level as well as the enterprise level to meet the board's needs. This is a key component of our ERM and governance model.

As this new COSO framework becomes finalized and broadly embraced, it will provide additional impetus for companies to adopt a broader ERM and governance framework such as what we have discussed.

Aligning Governance with ERM

Overall, we see companies continuing to need to align corporate governance with risk management. Directors, senior management, risk owners, internal auditors, and external auditors should know that ERM and governance processes must evolve continuously. The ERM and governance framework, responsibilities, and communications overlap, and one process affects the other. Everyone involved has important ERM and governance roles to play as they endeavor to more closely align their companies' governance with their ERM processes. ■

Paul J. Sobel, CPA, CIA, is vice president, internal audit, at Mirant Corporation, an energy company headquartered in Atlanta. He is the author of Auditor's Risk Management Guide: Integrating Auditing and ERM. *You can reach Paul at (678) 579-5042 or paul.sobel@mirant.com.*

Kurt F. Reding, Ph.D., CMA, CPA, CIA, is associate professor in the Department of Accounting at Pittsburg State University in Pittsburg, Kan. You can reach Kurt at (620) 235-4564 or kreding@pittstate.edu.

1 Thomas L. Barton, William G. Shenkir, and Paul L. Walker, *Enterprise Risk Management: Pulling it All Together*, the Institute of Internal Auditors Research Foundation, Altamonte Springs, Fla., April 2002, p. xi. Each of the five case studies in this study contains a segment on corporate governance.

2 Our definition of corporate governance is adapted from the Institute of Internal Auditors' definition of "governance process," which can be found in the IIA's *International Standards for the Professional Practice of Internal Auditing*. Our definition also incorporates ideas of effective corporate governance expressed in *Principles of Corporate Governance: A White Paper from the Business Roundtable*, Washington, D.C., May 2002. This publication describes the roles of the board of directors and management in corporate governance from a CEO's perspective.

3 Urton Anderson and Christy Chapman, *Implementing the Professional Practices Framework*, the Institute of Internal Auditors, Altamonte Springs, Fla., 2002, p. 112.

4 *Recommendations for Improving Corporate Governance*, the Institute of Internal Auditors, Altamonte Springs, Fla., 2002. The IIA offers and explains its recommendations for improving corporate governance in this position paper presented to Congress on April 8, 2002.

5 *Corporate Governance and the Board—What Works Best*, the Institute of Internal Auditors Research Foundation and Pricewater-

houseCoopers, Altamonte Springs, Fla., 2000, p. 12. Although this research study emphasizes corporate governance from the perspective of boards of directors, it offers many insights that other parties involved in corporate governance will find useful. Also see *Principles of Corporate Governance: A White Paper from the Business Roundtable*, May 2002, p. 1.

6 Barton, Shenkir, and Walker, April 2002, p. 121.

7 *Principles of Corporate Governance, A White Paper from the Business Roundtable*, May 2002, p. 16-17.

8 *Beyond Compliance: Building a Governance Culture*, the Joint Committee on Corporate Governance, the Canadian Institute of Chartered Accountants, Toronto, Ontario, Canada, November 2001. This report recommends that boards of directors involve themselves actively in risk management and describes responsibilities they should assume.

9 *Corporate Governance and the Board—What Works Best*, 2000, pp. 11-18.

10 Thomas L. Barton, William G. Shenkir, and Paul L. Walker, *Making Enterprise Risk Management Pay Off*, the Financial Executives Research Foundation, Florham Park, N.J., 2001. This research report does not emphasize corporate governance but does include relevant information such as companies' risk infrastructures that is helpful for tying governance and ERM concepts together.

11 Barton, Shenkir, and Walker, April 2002, p. 121.

12 Barton, Shenkir, and Walker, 2001, p. 29.

13 Barton, Shenkir, and Walker, April 2002, p. 70.

14 Barton, Shenkir, and Walker, 2001, p. 97.

15 Barton, Shenkir, and Walker, April 2002, p. 90-91.

16 *International Standards for the Professional Practice of Internal Auditing*, the Institute of Internal Auditors, Altamonte Springs, Fla. This publication is continuously updated online at http://www.theiia.org.

17 *Recommendations for Improving Corporate Governance*, April 8, 2002.

18 *Internal Control: Integrated Framework*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), 1992.

19 *Recommendations for Improving Corporate Governance*, April 8, 2002, and *Recommendations from the National Association of Corporate Directors to the House Committee on Energy and Commerce*, National Association of Corporate Directors, April 2002.

20 *Recommendations for Improving Corporate Governance*, April 8, 2002, and *Internal Control: Guidance for Directors on the Combined Code (the Turnbull Report)*, the Institute of Chartered Accountants in England & Wales, September 1999.

21 *Enterprise Risk Management Framework*, the Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2003.