

# DIRECTORS MONTHLY

February 2004  
Volume 28 Number 2

Reprinted with permission from the  
National Association of Corporate Directors (NACD)



## Pollution Risk Oversight

By Greg Rogers

Pollution risk oversight comprises the legal responsibilities of directors to provide oversight of the corporation's compliance with environmental laws, financial reporting of environmental liabilities, and management of environmental risk. This article begins with a general discussion of the board's risk oversight duties, then describes how these general responsibilities apply to the area of environmental management.

### Risk Oversight

Legal standards governing the responsibilities of corporate directors are undergoing a transformation as policy makers struggle to find solutions to perceived weaknesses in corporate governance. As a result, the role of the board of directors is fundamentally changing. Once, board members were expected to make major corporate decisions. As long as they were reasonably informed and acted without self-interest, directors were protected from being second-guessed on their decisions by the director-friendly business judgment rule.

### About NACD

**National Association of Corporate Directors (NACD)**, an independent not-for-profit organization founded in 1977, is the country's only membership organization devoted exclusively to improving corporate board performance. The NACD conducts educational programs and standard-setting research, and provides information and guidance on a variety of board governance issues and practices. Membership comprises board members from U.S. and overseas companies ranging from large publicly held corporations to small over-the-counter, closely held, and private firms. NACD lists all interested members on The Director's Registry, which is used by member companies and others that seek qualified directors. With chapters in many major cities providing educational programs and networking opportunities, NACD operates at both a national and local level. To educate the corporate community and to provide networking links among NACD members, the NACD holds an annual Corporate Governance Conference, where it presents a Director of the Year Award.



1828 L Street, NW  
Suite 801  
Washington, D.C. 20036  
202-775-0509  
[www.nacdonline.org](http://www.nacdonline.org)



Today, corporate directors are expected to do much more than make decisions. They are expected to proactively identify and address the significant risks facing the organization. The board's new "risk oversight" role is described in detail in the *Report of the NACD Blue Ribbon Commission on Risk Oversight* (2002). Before, the board was free to play a reactive role, dealing with problems and events as they arose. Now, the board is expected to have mechanisms in place to identify and manage risks before problems arise.

Historically, absent grounds to suspect deception, corporate boards were entitled to assume the integrity of management and employees and the honesty of their dealings on the company's behalf. Today, directors must assume the very opposite—that some employees will deliberately violate corporate policy and the law—and take steps to ensure that appropriate systems are in place to identify and appropriately respond to such situations on a timely basis. Whereas directors once were expected to rely on people, today directors are expected to rely on increasingly sophisticated mechanisms of control.

In the event that such mechanisms fail and problems arise anyway, what then? The business judgment rule cannot provide protection. After all, the board made no decision for which its business judgment can be second-guessed. Instead, the question is whether the board exercised appropriate risk oversight. The legal standards governing a director's fiduciary duty of care with respect to risk oversight are still in the early stages of development. However, the principles of internal control, which are well developed, provide the basis for answering the question that every director should now be asking, "What constitutes appropriate risk oversight?"

### Internal Control

At the heart of the transformation in the role of the board are the principles of "internal control" (used here to refer generally to compliance programs designed to ensure the achievement of organizational objectives), and the role that internal control can and should play in improving corporate governance. By now, most corpo-

rate directors probably have heard of the internal control requirements under Sections 302 and 404 of the Sarbanes-Oxley Act. What many directors may not realize is that internal control is not a specialized discipline applicable only to Securities and Exchange Commission (SEC) financial reporting. Internal control applies to all companies—public and private. It applies to nearly every area of management, including environmental compliance and risk management. Most importantly, it provides the foundation for understanding and fulfilling a director's fiduciary duty to provide effective oversight of corporate activities.

### The COSO Framework

The leading U.S. standard of internal control is the "COSO Internal Control-Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). This comprehensive framework remained largely unknown outside of the financial auditing profession from its release in 1994 until passage of the Sarbanes-Oxley Act. Regulations promulgated by the SEC implementing Section 404 of Sarbanes-Oxley (relating to internal controls) recognized the COSO Framework as a suitable framework for management to use in evaluating the company's internal control over financial reporting. Today, the COSO Framework is the *de facto* standard for U.S. companies implementing and evaluating internal control over financial reporting.

The COSO Framework describes five elements of internal control:

- *The control environment.* The control environment sets the tone of an organization. Relevant factors include, among other things, the attention and direction provided by the board of directors.
- *Risk assessment.* Risk assessment is the identification and analysis of relevant risks to achievement of the company's objectives.
- *Control activities.* Control activities are the policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
- *Information and communication.* The company must identify, capture, and communicate relevant information in a form and timeframe that enables people to carry out their responsibilities.
- *Monitoring.* The quality of the internal control system's performance over time must be monitored. This is accomplished through a combination of ongoing monitoring activities and separate evaluations.

**Director Summary:** Pollution risk oversight is the process by which board members attain reasonable assurance that the company's environmental-related objectives will be met. It comprises the legal responsibilities of directors to provide oversight of the corporation's compliance with environmental laws, financial reporting of environmental liabilities, and management of environmental risk.



## The legal standards governing a director's fiduciary duty of care with respect to risk oversight are still in the early stages of development.

Although the COSO Framework was developed for the primary purpose of preventing financial fraud, it is equally applicable to organizational compliance and risk management programs. The COSO Framework defines internal control as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in three categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Federal securities laws now require management and the company's independent auditor to certify that effective internal control over financial reporting is in place. Although they make no specific reference to internal control or the COSO Framework, several other recent legal developments affecting directors—of both public and private companies—impose requirements for various elements of internal control. Many of these developments focus on the board's responsibility to oversee the corporation's compliance with laws and regulations.

### Caremark International

As reported by the NACD's Blue Ribbon Commission on Risk Oversight, the benchmark for directors' risk oversight obligations was established in *In re Caremark International, Inc.*, a 1996 landmark Delaware decision. The derivative suit before the court involved claims that members of Caremark's board of directors breached their fiduciary duty of care to Caremark in connection with alleged violations by Caremark employees of federal and state laws and regulations.

The court noted that director liability for a breach of the duty to exercise appropriate attention may arise in two distinct contexts. First, such liability may follow from a board decision that results in a loss because that decision was ill advised or negligent. In such cases, liability is typically subject to the director-protective business judgment rule, assuming the decision made was the product of a process that was either deliberately considered in good faith or was otherwise rational.

Second, liability to the corporation for a loss may arise from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss. In such cases, corporate boards must satisfy their duty of care to be reasonably informed by:

assuring themselves that information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance.

The court in *Caremark* did not elaborate on the elements and characteristics of a "reasonable information and reporting system," stating only that the level of detail that is appropriate for such systems is a question of business judgment.

### Federal Prosecution of Business Organizations

In January 2003, in response to the rash of high-profile accounting scandals, the U.S. Department of Justice (DOJ) issued an internal guidance memorandum on "Principles of Federal Prosecution of Business Organizations." The guidance reiterated existing DOJ policy that the existence and adequacy of the corporation's compliance program should be considered as one of several factors in determining whether to bring criminal charges against a corporation. The guidance goes on to state, however, that the existence of a compliance program is not sufficient, in and of itself, to justify not charging a corporation for criminal conduct undertaken by its officers, directors, employees, or agents.

When evaluating compliance programs, prosecutors must consider whether the corporation has established corporate governance mechanisms that can *effectively* detect and prevent misconduct. The guidance cites as examples of such mechanisms the following:

- Do the corporation's directors exercise independent review over proposed corporate actions rather than unquestioningly ratifying officers' recommendations?
- Are the directors provided with information sufficient to enable the exercise of independent judgment?
- Are internal audit functions conducted at a level sufficient to ensure their independence and accuracy?
- Have the directors established an information and reporting system in the organization reasonably designed to provide management and the board of directors with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law (citing *Caremark*)?



While acknowledging that no compliance program can ever prevent all criminal activity by a corporation's employees, the DOJ guidance suggests that the commission of such crimes in the face of a compliance program may suggest that the board of directors is not adequately enforcing the program.

### Organizational Sentencing Guidelines

In determining the board's responsibility to oversee the corporation's compliance with laws and regulations, the court in *Caremark* placed considerable weight on the Organizational Sentencing Guidelines adopted in 1991 by the United States Sentencing Commission. The Guidelines, which set forth a uniform sentencing structure for organizations to be sentenced for violation of federal criminal statutes, offer powerful incentives for corporations to implement compliance programs to detect violations of law, promptly to report violations to appropriate public officials when discovered, and to take voluntary remedial efforts.

In October 2003, an Ad Hoc Advisory Group on the Guidelines recommended changes to give organizations greater guidance regarding the factors that are likely to result in "effective programs to prevent and detect violations of law." The Advisory Group paid special attention to the role of the organization's board of directors, recommending that the Guidelines be modified to provide that:

The organization's governing authority shall be knowledgeable about the content and operation of the program to prevent and detect violations of law and shall exercise reasonable oversight with respect to the implementation and effectiveness of the program to prevent and detect violations of law.

The Advisory Group concluded that this requirement is consistent with the views expressed in *Caremark*, namely that directors and officers have an obligation to become informed about the accuracy and timeliness of compliance reporting systems within their organizations in order to reach informed judgments about compliance with the law.

### NYSE Corporate Governance Rules

Under revised corporate governance rules recently adopted by the New York Stock Exchange (NYSE) and approved by the SEC, the audit committees of listed companies must have a written charter that defines the committee's purpose—which, at minimum, must be to assist board oversight of (1) the integrity of the company's financial statements, (2) the company's compliance with legal and regulatory requirements, (3) the independent

auditor's qualifications and independence, and (4) the performance of the company's internal audit function and independent auditors. The audit committee's responsibilities go beyond financial reporting and legal compliance to include risk assessment and risk management. The standards state that while it is the job of the CEO and senior management to assess and manage the company's exposure to risk, the audit committee must discuss guidelines and policies to govern the process by which this is handled. The audit committee must discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures.

### Pollution Risk Oversight

For the reasons described above, the principles of internal control are redefining the role of corporate directors. Environmental management happens to be an ideal application for internal control because it affects the achievement of organizational objectives in all three of the categories set forth in the COSO Framework: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Table 1 lists environmental-related objectives that organizations with material environmental liabilities and risks are likely to have, whether such objectives are formally stated or not. Pollution risk oversight is the process by which board members attain

**Table 1  
Environmental-Related Objectives**

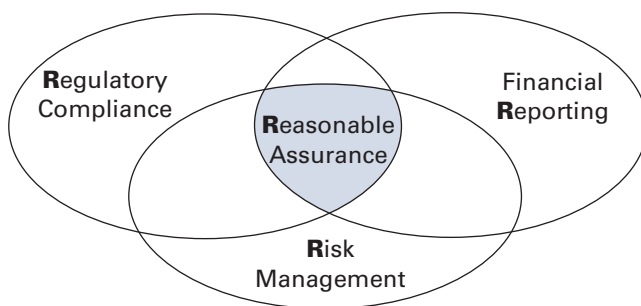
- Regulatory compliance.** The organization should achieve and maintain full compliance with applicable environmental laws, regulations, and permits;
- Financial reporting.** The financial statements should (i) comply with generally accepted accounting principles and specific SEC reporting requirements for environmental matters, and (ii) fairly present the company's financial conditions taking into account environmental liabilities and risks; and
- Risk management.** The company should identify environmental-related risks that could have a material adverse impact on achievement of its financial and operational objectives, and take timely and appropriate action to control and finance these risks.



reasonable assurance that the company's environmental-related objectives will be met.

As illustrated in Figure 1, a company's environmental-related objectives in the areas of regulatory compliance, financial reporting, and risk management may be closely interrelated. For example, a company's failure to properly account for environmental remediation liabilities under generally accepted accounting principles may also represent a violation of law or contract (such as a loan covenant), and the availability of environmental insurance may affect the degree of necessary financial disclosure. Likewise, many of the same internal control components will serve to achieve multiple objectives. For example, systematic identification of environmental loss exposures is a first step toward complying with environmental laws, advising shareholders of material environmental liabilities and risks, and acquiring appropriate insurance coverage to protect the organization and its directors and officers from environmental-related losses.

**Figure 1. The Four Rs of Pollution Risk Oversight**



### Board Action

The emerging prominence of internal control and its role in corporate governance raises several important questions for directors in evaluating their pollution risk oversight responsibilities. For example:

- How does a director become knowledgeable about the content and operation of environmental internal control systems?
- What is a director's responsibility with respect to the design and implementation of such systems?
- How can a director gain reasonable assurance that the company's system is effective?

In view of *Caremark* and other recent developments, the board is obligated to exercise reasonable oversight with respect to the implementation and effective operation of a framework of internal control to provide reasonable assurance that the company's environmental

## The audit committee must discuss the company's major financial risk exposures and the steps management has taken to monitor and control such exposures.

objectives are achieved. Directors can become generally knowledgeable about the content and operation of internal control systems by reviewing the COSO Framework and the other governing standards described in this article. Consultation with environmental specialists will be needed to understand how these general internal control guidelines can be applied to support a company's environmental objectives.

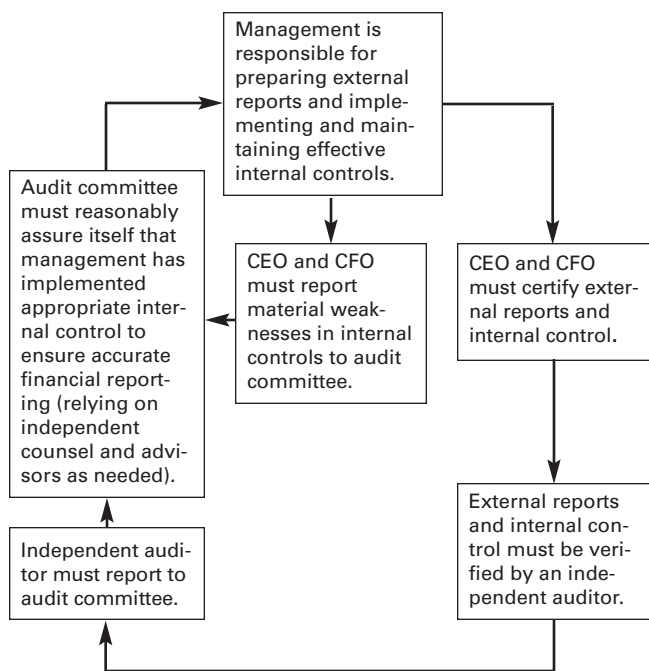
The board must next determine its responsibilities with regard to the design, implementation, and effective operation of the internal control system. Figure 2 (on page 6) illustrates the model set forth in Sarbanes-Oxley by which the audit committee is to provide oversight of financial reporting. This "assurance model" defines the respective roles of the audit committee (leadership and risk oversight), management (internal control system design, implementation, and operation), and the financial auditor (independent verification of system design and operational effectiveness). Significantly, Sarbanes-Oxley requires that the independent auditor be retained by and report to the audit committee, not management.

The assurance model depicted in Figure 2 is statutorily required for SEC reporting purposes under Sarbanes-Oxley. In addition, the new NYSE listing standards suggest that this model should be applied more broadly to oversight of compliance with legal and regulatory requirements and risk management. For now, even where it may not be legally required—for example, in the case of privately held companies or with respect to non-regulatory matters—the assurance model establishes "best practice" for fulfilling the board's pollution risk oversight responsibilities with respect to all three internal control objectives: compliance with environmental laws and regulations, environmental financial reporting, and environmental risk management. In the future, as courts attempt to further define the board's oversight responsibilities generally described in *Caremark*, the assurance model in Figure 2 may become the new legal standard of care for risk oversight.



## Pollution risk oversight is the process by which board members attain reasonable assurance that the company's environmental-related objectives will be met.

Figure 2. Sarbanes-Oxley Assurance Model



Using the assurance model in Figure 2 as a guide, corporate directors in industries with significant environmental exposures can take the following steps in fulfilling their pollution risk oversight responsibilities:

- Define the organization's environmental-related objectives (relying on independent counsel and advisors as needed);
- Direct management to implement a system of internal control reasonably designed to ensure achievement of these objectives;
- Actively fulfill the board's assigned role in the implementation and ongoing operation of the internal control system; and
- Retain an independent auditor to periodically evaluate the internal control system and attest to its design and operational effectiveness.

### Conclusion

Legal standards governing the responsibilities of corporate directors are undergoing a transformation. Today, corporate directors are expected to proactively identify and address the significant risks facing the organization. Before, the board was free to play a reactive role, dealing with problems and events as they arose. Now, the board is expected to have mechanisms in place to identify and manage risks before problems arise. Such mechanisms are the subject of internal control.

Internal control is not limited to financial reporting. For companies in industries with significant environmental exposures—including oil and gas, refining, utilities, mining, chemicals, manufacturing, printing, transportation, and waste management—it has direct application to environmental compliance and risk management, as well as environmental financial reporting. Internal control provides the foundation for understanding and fulfilling a director's fiduciary duty to provide effective pollution risk oversight. To fulfill their oversight responsibilities, corporate directors must understand the principles of internal control and the process by which the board can reasonably assure itself that effective internal control is in place. ■

**Greg Rogers, JD, CPA**, practices environmental law at Guida, Slavich & Flores, P.C., in Dallas. His e-mail is [rogers@guidaslavichflores.com](mailto:rogers@guidaslavichflores.com).