Chapter 6

Oversight, Compliance, and Risk Management

6.1 The New Regulatory Climate

Complying with the new regulations has not only dramatically increased the workload and responsibilities of CFOs, finance teams, and directors, but it also has fundamentally changed their role and their relationship with other, nonfinancial groups within the corporation. For example, the provisions of the Sarbanes-Oxley Act call for senior finance executives and the audit committee of the board to take a much more active role in the operations of the business, as they are charged with certifying the strength of both a company's internal controls and the information they generate. Three sections of Sarbanes-Oxley are especially relevant: section 302, which outlines corporate responsibility for financial reports; section 404, which covers management assessment of internal controls; and section 409, which requires more rapid public disclosure of so-called material events in company performance.

Traditionally, the role of the *audit committee* has been to oversee, monitor, and advise company management and outside auditors in conducting audits and preparing financial statements, subject to the ultimate authority of the board of directors. The Securities and Exchange Commission (SEC) first recommended that publicly held companies establish audit committees in 1972. The stock exchanges quickly followed suit by either requiring or recommending that companies establish audit committees. In 2002, Sarbanes-Oxley increased audit committees' responsibilities and authority, and raised membership requirements and committee composition to include more independent directors. The SEC and the stock exchanges followed with additional new regulations and rules to strengthen audit committees.Keinath and Walo (2004), p. 23.

Fulfilling all of the duties and responsibilities assigned to them under recent legislation and newly adopted stock exchange rules and shifting to a more proactive **oversight**[1] role represent major challenges for audit committees. Their responsibilities have been expanded in major ways and now include ensuring accountability on the part of management and internal and external auditors; making certain all groups involved in the financial reporting and internal controls process understand their roles; gaining input from the internal auditors, external auditors, and outside experts when needed; and safeguarding the overall objectivity of the financial reporting and internal controls process.

1. Regulatory review, monitoring, and supervision used in reporting and monitoring internal controls.

Importantly, in the wake of Sarbanes-Oxley, the relationship between management and outside auditors has been replaced by one between the audit committee and outside auditors. The audit committee now is directly responsible for appointment, compensation, retention, and oversight of independent auditors who report

directly to the audit committee. And, by vesting responsibility and authority for certain audit-related actions in the audit committee—to the exclusion of the full board, management, and shareholders—Sarbanes-Oxley appears to alter the traditional delegation, under state law, of board power to a committee.

The audit committee must also establish specific procedures for handling complaints received by the company regarding accounting, internal accounting controls, or auditing matters, including confidential submission by company employees of concerns regarding questionable accounting or auditing matters. In addition, all audit services and permitted nonaudit services provided by outside accounting firms must be preapproved by the audit committee. All approvals of nonaudit services must also be disclosed in the company's periodic reports. Certain nonaudit services by firms that perform audits are expressly prohibited.

As noted in Chapter 4 "Recent U.S. Governance Reforms", the composition and credentials of the audit committee are also tightly regulated. Public companies are required to have an audit committee consisting of at least three independent members of the board of directors. Each committee member must be "financially literate" and at least one member must be designated as the "financial expert," as defined by applicable legislation and regulation.

Audit committees are required to define their responsibilities and operations in an *audit committee charter*.For an example of an audit committee charter, consult the Web site of any major public corporation., This section is based on The Institute of Internal Auditors (2006), "The Audit Committee—Purpose, Process, Professionalism." http://www.theiia.org Such a charter should (a) clearly delineate audit committee processes, procedures, and responsibilities that have been sanctioned by the entire board; (b) define membership requirements, including a provision for a financial expert; (c) allow for yearly reviews and changes; (d) designate the minimum number of meetings to be conducted; (e) accommodate executive sessions with appropriate entities and allow for engaging outside counsel as needed; (f) outline the committee's responsibilities in regard to risk management, compliance issues, and review of its own effectiveness; identify the specific areas the audit committee should review as well as with whom those reviews will be conducted; and include such specific roles as annual report preparation oversight and yearly agenda planning; and (g) delineate the audit committee's relationships with the internal and external auditors; appoint, evaluate, set time limits for, and discharge (with the concurrence of the full board) the external auditors; and evaluate the independence of both the internal and external auditors.

6.2 Warren Buffett on the Challenge of the Audit Committee

Often called the "Oracle of Omaha," Warren Buffett, the largest shareholder and CEO of Berkshire Hathaway, is well known for his adherence to the value investing philosophy, his conservatism when it comes to issues of governance and accounting, and for his personal frugality, despite his immense wealth. On the subject of a board's audit committee, he writes,Buffett, annual letter to Berkshire Hathaway shareholders (2002).

Audit committees can't audit. Only a company's outside auditor can determine whether the earnings that a management purports to have made are suspect. Reforms that ignore this reality and that instead focus on the structure and charter of the audit committee will accomplish little.

As we've discussed, far too many managers have fudged their company's numbers in recent years, using both accounting and operational techniques that are typically legal but that nevertheless materially mislead investors. Frequently, auditors knew about these deceptions. Too often, however, they remained silent. The key job of the audit committee is simply to get the auditors to divulge what they know.

To do this job, the committee must make sure that the auditors worry more about misleading its members than about offending management. In recent years, auditors have not felt that way. They have instead generally viewed the CEO, rather than the shareholders or directors, as their client. That has been a natural result of day-to-day working relationships and also of the auditors' understanding that, no matter what the book says, the CEO and CFO pay their fees and determine whether they are retained for both auditing and other work. The rules that have been recently instituted won't materially change this reality. What *will* break this cozy relationship is audit committees unequivocally putting auditors on the spot, making them understand they will become liable for major monetary penalties if they don't come forth with what they know or suspect.

In my opinion, audit committees can accomplish this goal by asking four questions of auditors, the answers to which should be recorded and reported to shareholders. These questions are:

1. If the auditor were solely responsible for preparation of the company's financial statements, would they have in any way been prepared differently from the manner selected by management? This question should cover both material and nonmaterial differences. If the auditor

would have done something differently, both management's argument and the auditor's response should be disclosed. The audit committee should then evaluate the facts.

2. If the auditor were an investor, would he have received—in plain English—the information essential to his understanding the company's financial performance during the reporting period?
3. Is the company following the same internal audit procedure that would be followed if the auditor himself were CEO? If not, what are the differences and why?
4. Is the auditor aware of any actions—either accounting or operational—that have had the purpose and effect of moving revenues or expenses from one reporting period to another?

If the audit committee asks these questions, its composition—the focus of most reforms—is of minor importance. In addition, the procedure will save time and expense. When auditors are put on the spot, they will do their duty. If they are not put on the spot... well, we have seen the results of that.

6.3 Legal Issues Regarding Oversight

Much has been written about the board of directors' *Duty of Care* in the *decision-making* context, which requires directors to perform their duties in good faith and with the degree of care that an ordinary person would use under similar circumstances. Most directors are similarly aware of the protections afforded by the *Business Judgment Rule*—courts will not second guess directors' business decisions if the directors act on an informed basis and in good faith. By contrast, the *oversight* role of the board is less well defined from a legal perspective. The reason is that, in an oversight context, directors are not protected by the Business Judgment Rule if they fail to take action when they become aware of corporate impropriety. Many directors are unfamiliar with this less defined and stricter component of the Duty of Care.This section is based on Kleinman and Thompson (2002).

In adjudicating claims, the law distinguishes between two scenarios: deciding there is no problem and ignoring a problem. When a board considers a situation and makes a decision that results in a loss, the Business Judgment Rule will protect a board's decision if the board acted in good faith and properly informed itself in the process. The protection of the Business Judgment Rule is not determined by the results of the decision but by the quality of the process employed. For example, when a board conducts a proper investigation and either takes action or consciously decides that action is not necessary, that decision, even if wrong, will be protected by the Business Judgment Rule.

By contrast, when a loss occurs because of a board's failure to consider a problem, there has been no process, there is no decision to protect, and the Business Judgment Rule does not apply. Instead, directors may face liability for breach of the *Duty of Oversight*. Rather than having a court defer to the directors' business judgment, the directors will likely be required to defend a negligence claim. Thus, when directors are aware, or should be aware, of material improper conduct, violations of law or other action that could result in material harm to the organization, the Duty of Oversight demands that directors investigate the matter and decide whether or not corrective action is needed. If the board fails to consider the situation, the board will be criticized for failure to supervise and may face liability under the Duty of Oversight. Specifically, boards can be held liable under the Duty of Oversight for failing to act when they know or *should know* of wrongdoing.The leading Delaware cases addressing the duty of oversight and related issues are *Graham v. Allis-Chalmers Mfg. Co.* (1963); *In re Caremark International Derivative Litigation* (1996); *Aronson v. Lewis* (1984); *Boeing Co. v. Shrontz* (1992); and *In re Dataproducts Corp. Shareholders Litigation* (1991). See also Hansen (1993).

Note that although the board may not take action in either case, the results in the two cases are dramatically different. The Duty of Oversight, therefore, creates an incentive for boards to respond to potential indications of wrongdoing in order to gain the benefit of the Business Judgment Rule.

How can a board protect itself? The law demands that directors investigate when there are red flags. If a director has actual knowledge of a material problem, he or she would be well advised not to wait for management to bring the topic before the board. Proper board action will always be the best defense to a Duty of Oversight claim.

Delaware law allows a corporation, in its certificate of incorporation, to eliminate or reduce the personal liability of directors for breaches of fiduciary duty, including the Duty of Care. Although the Duty of Oversight is considered a component of the Duty of Care, Delaware courts have not specifically held that such a charter provision would bar a Duty of Oversight claim.

6.4 Red Flags in Management Culture, Strategies, and Practices

Analysis of corporations that have experienced major ethical and financial difficulties shows these companies have a great deal in common in terms of their corporate culture and management profiles, as well as their accounting and governance practices. On the basis of this knowledge, we can identify a number of early warning signals or red flags that boards can use to spot the emergence of a corporate environment and culture susceptible to conflicts of interest and management abuse. For a suggestive list, see Chapter 13 "Appendix B: Red Flags in Management ".This section is based on Wood (2005).

Individually, these factors may not be predictive of future problems. In groups, however, they define a heightened risk profile and should be cause for additional scrutiny and objective analysis. For example, the combination of aggressive management practices creating rapid short-term revenue and stock-price growth coupled with weak board oversight, allowing the CEO to rapidly accumulate personal wealth through stock-based incentive compensation, has been present in a significant percentage of recent problem situations. Risk of rapid financial deterioration in such cases is exacerbated when the company also operates with aggressive financial practices and high leverage.

Audit committees would be well advised to monitor these categories of higher risk characteristics based on their proven usefulness in identifying corporate environments that may be susceptible to rapid stock price and credit deterioration, as well as fraud.

6.5 Questions About Ethics and Compliance for the Board

Building a culture of ethics and compliance is an imperative for today's board directors. This requires senior management involvement, organization-wide commitment, an effective communications system, and an ongoing monitoring system. To ensure total commitment, directors must ask the right questions that will assist them in assessing whether an effective program is in place. The following set of questions is suggested as a starting point:

1. Does the tone at the top, as communicated by senior management, demonstrate to every employee that ethics and compliance are vital to continued business success? Does the organization's culture support making ethical and compliant choices?
2. How has the organization supported the ethics and compliance program through training and communication efforts?
3. Can you describe the process for assessing ethics and compliance risks within the organization? Has the organization ever performed a cultural assessment?
4. How is the current ethics and compliance program structured? Does it cover the organization's global operations? Has it addressed the high-priority areas? Has the organization's ethics and compliance program and code of ethics or conduct been updated to comply with the requirements of Sarbanes-Oxley? Has the organization reevaluated its internal reporting mechanisms in light of Sarbanes-Oxley?
5. Does the organization have an **ethics and compliance officer**[2]? Is a senior executive with adequate time, financial resources, and board access in charge of the program? Are there dedicated, full-time resources?
6. Does the ethics code include statements regarding responsibilities to employees, shareholders, suppliers, customers, and the community at large, and is it distributed to all relevant parties, including the board, employees, management, and vendors?
7. Does a reporting process exist to keep the board informed on ethics and compliance issues, as well as the actions taken to address those issues? Is ethics and compliance a regular board agenda item?
8. Is there an effective and utilized reporting mechanism in place to let all employees raise ethics and compliance issues without fear of retribution? Is there an anonymous reporting mechanism or helpline? Who fields the follow-ups on concerns raised through the helpline? Are audit committee members or the audit chair named as an additional outlet for employee concerns?

2. A senior executive within a corporation who is charged with ensuring that the company and the individuals it employs behave ethically and in ways that help the company succeed.

9. What type of ongoing monitoring and auditing processes are in place to assess the effectiveness of the program? Are the code of ethics and compliance program reviewed at least annually by senior management to determine if they need updating due to business, legal, or regulatory changes? Does the internal audit function conduct reviews? Are employee surveys conducted? Has the program been reviewed by outside consultants or experts for possible improvement?
10. Does the organization regularly and systematically scrutinize the sources of compliance failures and react appropriately? Does management take action on reports? Are employees appropriately and consistently disciplined?

6.6 Questions About Hedging, Derivatives, and Trading Risks

Increasingly, companies engage in hedging, derivative, and trading activities that involve substantial risks as part of their overall corporate strategy. Although hedging activities, with derivatives or other tools, may mitigate or resolve risky positions, hedges are rarely perfect. In addition, because of the sophisticated nature of hedging, derivative, and trading activities, the risk exposure of a company is difficult to define, complicating oversight of such activities by a board of directors.

At minimum, the board of a company engaging in hedging, derivative, or trading activities should ask the following questions:

1. Where are the hedging, derivative, and trading risks embedded in the company, and who in the company is responsible for these activities?
2. Does the board of directors understand the nature and purposes of the risk positions being taken?
3. Are there risk limitations in place, and, if so, what are they and how effectively are they implemented?
4. What is the risk to reward ratio that fits into the company's strategic plan?
5. Does the board of directors have a glossary to translate the explanations that it is likely to receive?

6.7 Enterprise Risk Management: The Board's New Tool

Whereas traditional **risk management**[3] approaches focus on protecting a company's tangible assets and the related contractual rights and obligations, the scope of a new approach called **Enterprise Risk Management (ERM)**[4] is much broader. ERM, discussed in greater detail in Chapter 14 "Appendix C: Enterprise Risk Management: Ask the Board ", is more than crisis management or regulatory compliance. It is a tangible and structured approach to addressing organizational and financial risk. It is strategic in focus, aimed at enhancing and protecting a company's tangible and intangible assets on an enterprise-wide basis. Its basic premise is that uncertainty presents both risk and opportunity, with the potential to erode or enhance value. Value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives.For a more detailed discussion of this subject, see Waller, Lansden, Dortch, and Davis (2005) and Chapter 14 "Appendix C: Enterprise Risk Management: Ask the Board ".

Although the management of a company is ultimately responsible for a company's risk management, the board of directors must understand the risks facing the company and oversee the risk-management process. Best practice suggests that board committees should incorporate risk management into their charters. A company's governance and nominating committee, for example, 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 and nominating committee should also work with management to establish an orientation program for new directors and succession plans for key executive officers.

More commonly, however, corporate governance guidelines delegate the responsibility for risk management 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.

3. A traditional approach that focuses on protecting a company's tangible assets and the related contractual rights and obligations.
4. A risk management approach that is more structured and strategic than traditional risk management. ERM is aimed at enhancing and protecting a company's tangible and intangible assets on an enterprise-wide basis.

6.8 Codes of Ethics and Codes of Conduct

In 2003, to implement sections 406 and 407 of Sarbanes-Oxley, the SEC adopted a rule requiring a company to disclose whether it has adopted a code of ethics that applies to the company's principal executive officer, principal financial officer, principal accounting officer or controller, or persons performing similar functions. A company disclosing that it has not adopted such a code must disclose this fact and explain why it has not done so. Companies also are required to promptly disclose amendments to, and waivers from, the code of ethics relating to any of those officers.

A **code of ethics**[5] (code of conduct, statement of business practice, or a set of business principles) is useful for establishing and articulating the corporate values, responsibilities, obligations, and ethical ambitions of an organization and the way it functions. It provides guidance to employees on how to handle situations that pose a dilemma between alternative, right courses of action or when faced with pressure to consider right and wrong.

A good code of ethics should be signed by the CEO and endorsed by the board of directors; it should focus on the values that are important to top management in the conduct of the business, such as integrity, responsibility, and reputation, and demonstrate a commitment to maintaining high standards both within the organization and in its dealings with others.

A good example is the code of ethics authored by Buffett for Berkshire Hathaway directors, executives, and employees, with his now famous advice:

I want employees to ask themselves whether they are willing to have any contemplated act appear the next day on the front page of their local paper—to be read by their spouses, children and friends—with the reporting done by an informed and critical reporter.Web site of Berkshire Hathaway, available at http://www.berkshirehathaway.com.

5. A code of conduct, a statement of business practice, or a set of business principles that establish and articulate a company's values, responsibilities, obligations, and ethical ambitions.