Susan S Bies: Effective corporate governance and the role of counsel

Remarks by Ms Susan Schmidt Bies, Member of the Board of Governors of the US Federal Reserve System, at the Annual Meeting of the American Bar Association, San Franciso, California, 10 August 2003.

* * *

Good morning. Thank you for the invitation to speak to the American Bar Association about a subject that has been in the spotlight in the business community the past two years. This morning I would like to make a few remarks about the role that legal counsel and other professionals should play in ensuring effective corporate governance.

The problems associated with companies such as Enron, HealthSouth, and WorldCom, to name a few, have caused lawmakers, regulators, managers, and directors to dramatically increase their attention to internal controls, accounting policies, risk management, and corporate governance procedures. At government agencies, a great deal of time and effort has gone into reviewing and clarifying standards of how companies should implement these basic functions. Within industry, corporate leaders have worked to enhance existing controls and procedures to address these areas. Much has been accomplished, but still more needs to be done in today's changing environment.

Some of the most high-profile problems reported in the media have caused us to step back and ask, “How did this happen?” We've seen some astonishing corporate governance and internal control breakdowns in companies that exhibited no outward indication of serious problems. In some cases it appears that critical internal controls were treated as very low priorities or simply ignored altogether.

In a number of cases, regulatory or law enforcement actions precipitated the very active involvement of rafts of highly capable outside professionals, including auditors, consultants, and attorneys, to investigate and address the identified issues. It is fair to ask why those resources and expertise were absent earlier in the risk-management processes, when more diligent attention to fundamental principles could have helped companies and their shareholders avoid serious reputational and financial harm.

I would like to talk about the role the legal community can play in ensuring that the important basic elements of risk management and internal controls are effectively addressed on a proactive basis, rather than after problems arise. First I will describe some problems we have recently seen at financial institutions. Then I will provide a suggested framework for effective internal controls and compliance in the context of good corporate governance. Finally, I will outline some specific enforcement actions we have recently taken that relate to effective legal and reputational risk management.

Examples of some current problems at financial institutions

As a member of the Federal Reserve Board and the Chair of the Board's Committee on Supervisory and Regulatory Affairs, I've seen several problem situations recently that have been the result of weak internal control environments, poor accounting practices, inadequate corporate governance mechanisms, or less-than-thorough risk-management procedures.

Here are some examples of notable recent situations that have come to our attention and in some instances to the attention of the press and the public. These particular fact patterns relate to financial institutions, but the underlying corporate governance issues have wider application.

- We have seen instances where inadequate anti-money laundering programs permitted criminals to launder funds through banks. The programs had deficient audit and management oversight, and did not receive an appropriate level of compliance and legal review.
- In a couple of cases, failures to segregate duties enabled individuals to commit fraud by entering false information into a bank's books and records or by accessing the general ledger and authorizing fraudulent funds transfers.

- In one case, grossly inadequate management oversight resulted in the operation of a trading program with numerous phony transactions. This extended over a period of years, causing significant financial losses to the financial institution.
- A repeated problem is inadequate management and audit committee oversight of business lines. In one case, this resulted in an institution engaging in transactions with special purpose entities without adequate director knowledge and without effective identification and management of risks.
- Despite apparent approval by outside auditors and lawyers, we have seen transactions that elevated form over substance, transgressed accounting rules, created serious reputational and legal risk for the institution and ultimately resulted in serious sanctions. During the subsequent investigations, moreover, facts surfaced that raised serious questions about the independence of the outside professionals engaged to provide crucial advice.
- Finally, we have seen banking organizations enter into novel, complex financial transactions, driven almost entirely by business line managers, without adequate review by supporting areas and without full consideration of attendant risks.

In the course of our review of these situations, we found that the banking organizations subject to the Board's enforcement actions generally had no hesitation in securing the assistance of experienced and qualified counsel to represent them during the discussions with the Board's supervision and enforcement staff. However, that expertise often was apparently not consulted *before* the problems became so severe that formal, public corrective action became necessary. This failure raises several questions: Did these financial institutions properly utilize their in-house and outside counsel? Did companies' counsel get involved, did they perform poorly, or did management ignore their advice? Alternatively, are current legal standards and practices inadequate to address the types of problems that are now arising in these very important areas?

I don't believe there is a single answer that applies in each case, but as a general matter, we may conclude that in each case the institution failed to give risk management the appropriate attention and resources until it was too late to fix the problems without significant financial or reputational damage. Therefore, a clear priority for companies should be to refocus on the basics of internal controls and risk management, and to review how these basics should be applied from the inception of projects rather than in hindsight. I'd like to mention a few principles of good corporate governance that particularly apply to the effective use of professional expertise, whether in-house or independent.

Internal control fundamentals

A mainstay of standards on internal controls is the report of the Committee of Sponsoring Organizations (COSO) titled *Internal Control--Integrated Framework*.[1] The report 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…:

- effectiveness and efficiency of operations,
- reliability of financial reporting, and
- compliance with applicable laws and regulations.”

The COSO model served as the basis for the internal control assessment and reporting requirements that have applied to depository institutions as part of the Federal Deposit Insurance Corporation Improvement Act since 1991, and that now are broadly applicable to public companies under the Sarbanes-Oxley Act.

In July, COSO issued draft guidance on enterprise risk management (ERM), which identifies all of the aspects that should be present in an enterprise risk management framework and describes how they

[1] Internal Control--Integrated Framework, *available from the American Institute of Certified Public Accountants, Order Department, Harborside Financial Center, 201 Plaza Three, Jersey City, NJ 07311-3881; www.coso.org*

can be implemented. It also identifies the interrelationships between risk and ERM, and the COSO Internal Control framework. The guidance defines enterprise risk management as:

…a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

As in-house or outside legal counsel, you are one of the “other personnel” referred to in this definition. As such, you will likely be part of the company's team that will implement ERM. I strongly encourage you to become familiar with your role in this process as outlined in the draft guidance. Since the guidance is currently out for a ninety-day comment period, which ends on October 14, 2003, I also encourage you to provide comment to COSO.[2]

The COSO internal control framework provides a comprehensive approach that is versatile enough to apply to organizations of all sizes and complexity. COSO requires all managers to, at least once a year, step back from their other duties and evaluate risks and controls within their scope of authority. Each manager should consider current and planned operational changes, identify risks, determine appropriate mitigating controls, establish an effective monitoring process, and evaluate the effectiveness of those controls. Managers then should report their assessment up the chain of command to the chief executive officer, with each new level of management in turn considering the risks and controls under its responsibility. The results of this process are ultimately reported to the audit committee of the board of directors. In the case of banks with assets greater than $500 million, management publicly reports on its assessment of the effectiveness of controls over financial reporting and the external auditor is required to attest to this self-assessment - a process that soon will be in place for public companies as well. Thus, the process helps managers communicate among themselves and with the board about the dynamic issues affecting risk exposures, risk appetites, and risk controls throughout the company.

Risk assessments such as the one outlined in COSO presumably could also be useful in assessing various lines of business when formulating business strategies. But not all corporations and boards consider risk during their annual strategic planning or other evaluation processes. The 2002 survey of corporate directors conducted jointly by the Institute of Internal Auditors and the National Association of Corporate Directors showed that directors were not focusing on risk management. I was surprised to learn that 45 percent of directors surveyed said their organization did not have a formal enterprise risk-management process - or any other formal method of identifying risk. An additional 19 percent said they were not sure whether their company had a formal process for identifying risks. These percentages indicate that some companies have directors who don't understand their responsibilities as the representatives of shareholders. The shareholders of those companies should be asking the directors how they govern an organization without a good understanding of the risks the company is facing and without knowledge of a systematic approach to identifying, assessing, monitoring, and mitigating excessive risk-taking. I trust that none of the directors who participated in the survey were on the board of a financial services company.

Although directors are not expected to understand every nuance of every line of business or to oversee every transaction, they do have responsibility for setting the tone regarding their corporations' risk-taking and establishing an effective monitoring program. They also have responsibility for overseeing the internal control processes, so that they can reasonably expect that their directives will be followed. They are responsible for hiring individuals who have integrity and can exercise sound judgment and are competent. In light of recent events, I might add that directors have a further responsibility for periodically determining whether their initial assessment of management's integrity was correct.

The COSO framework and the internal controls annual report process can be effective tools for management and the auditor to communicate risks and control processes to the audit committee. Members of that committee should use the reports to be sure business strategy, changing business processes, management reorganizations, and positioning for future growth are conducted within the

[2] Copies of the draft may be obtained on the web site at www.erm.coso.org.

context of a sound system of internal controls and governance. The report should identify priorities for strengthening the effectiveness of internal controls.

Indeed, beyond legal requirements, boards of directors of all firms should periodically assess the adherence by management, which has stewardship over shareholder resources, to ethical business practices. They should ask, for example: “Are we getting by on technicalities, adhering to the letter but not the spirit of the law? Are we compensating ourselves and others on the basis of contribution, or are we taking advantage of our positions? Would our reputation be tainted if word of our actions became public?” Legal professionals, whether in-house or outside counsel, can help direct management to focus on these kinds of questions. They can also help ensure that processes are in place for employees to raise ethical and compliance concerns in an environment that protects them from retribution from affected managers.

Internal controls over compliance

While much of the public attention around Sarbanes-Oxley focuses on the first two areas of the COSO framework - operations and financial reporting, counsel especially should not forget about the third area, “compliance with applicable laws and regulations.” Risk management clearly cannot be effective within a company if we forget about the basics of internal controls. It is worth stating that many of the problems at the heart of those headline cases stemmed from violations of the fundamental tenets of internal control, particularly those pertaining to operational risks. Based on the headlines, it seems that boards of directors, management, auditors, and counsel need a remedial course in Internal Controls 101. As corporations grow larger and more diverse, internal controls become more, not less, important to the ability of management and the board to monitor activity across the company.

The basics of internal controls for directors and managers are simple. Directors do not serve full time, so it is important that they establish an annual agenda to focus their attention on the high-risk and emerging-risk areas while ensuring that there are effective preventive or detective controls over the low-risk areas. A board of directors has the responsibility to understand the legal, reputational, and compliance risks facing an organization; legal professionals can assist in identifying those risks, quantifying them, and providing expertise in managing them.

Before a company moves into new and higher-risk areas, the boards of directors and management need assurances that the organization's governance practices are sound and effective. Many of the organizations that have seen their reputations tarnished in the past few years have neglected to consider emerging conflicts of interest when the organization adds new products and lines of business. For example, if a customer service or control function must be done in an independent, fiduciary, or unbiased manner relative to other activities, appropriate firewalls must be in place before the product or activity begins.

Internal controls and compliance are the responsibility of line managers, who must determine the acceptable level of risk in their line of business and assure themselves that the combination of earnings, capital, and internal controls is sufficient to compensate for the risk exposures. However, supporting functions such as legal, accounting, internal audit, and risk management should independently monitor the control processes to ensure that they are effective and that risks are measured appropriately. The results of these independent reviews should be routinely reported to executive management and boards of directors. Directors should be sufficiently engaged in the process to determine whether these reviews are in fact independent of the operating areas and whether the officers conducting the reviews can speak freely. Where it appears that supporting functions have not been sufficiently involved, directors must demand that management adjust the processes as necessary. If the in-house legal, accounting, or audit staff believes that a supporting function has not been given adequate information or opportunity for consultation, it must bring this deficiency to the attention of the board.

Sarbanes-Oxley Act

Now let's turn to Sarbanes-Oxley. I am not going to dwell on the specifics of the Act. You most likely already know the details of this important piece of legislation including, in particular, the provisions directly affecting attorneys practicing before the Securities and Exchange Commission. What I'd like to focus on is the purpose of the Act. At its core, the Sarbanes-Oxley Act is a call to return to the basics

that we have been discussing. Simply stated, the current status quo for corporate governance is unacceptable and must improve.

This message is applicable to both public and private companies alike and affects everyone within a company, as well as outside professionals hired by the company. As in-house or independent counsel you should fulfill your duties with the competence, integrity, and independence expected of members of the bar and be sure that any material concerns that you have concerning the company's conduct are raised to appropriate levels within the organization.

On a broader level, the role for legal counsel, in-house and outside, also is to ensure that the client understands the messages of Sarbanes-Oxley and that all areas within a company are taking appropriate steps to fulfill their obligations. To accomplish this task, legal professionals must become engaged in the mechanisms of internal controls, ensure that they receive prompt, comprehensive information from management, and have adequate access to the appropriate level of management and the board to be able to offer useful and timely counsel.

The role of legal professionals

In many recent cases, including the fact patterns I described a little earlier, companies did not take adequate steps to prevent the problem behavior in the first instance, and the companies' accountants, auditors and counsel were not asked to assist, were not able to assist, or were simply not actively engaged in foreseeing, identifying or addressing problems as they developed.

As legal representatives to various corporate entities, you are charged with making sure that your clients understand the basic need to put into place strong internal controls, state-of-the art accounting practices, and robust corporate governance systems. You also need to make sure that your clients understand potential corporate and individual liabilities in the event that basic functions are not adequately performed.

Professionals such as yourselves can do a number of things to participate in effective corporate governance. When a problem rises to the level of a formal enforcement action, we give institutions a lot of fairly detailed direction on how to improve internal controls and risk management, and professionals generally have a very important role in making these improvements.

In some of our recent public actions we have required financial institutions to take steps to ensure that legal and reputational risks are adequately addressed, and these steps all involve or have the potential to involve legal professionals. We have required institutions to establish controls that include the following:

- a formal policy that addresses tolerance for legal and reputational risks, including regular reassessments of risk tolerance by appropriate senior management;
- procedures for assessing legal and reputational concerns and, where appropriate, escalating them to appropriate levels of senior management;
- transaction approval and monitoring procedures that involve all relevant areas, including legal; and that everyone in the process receive complete information about the transaction, including the counterparty's purpose;
- appropriate due diligence on control processes at the institution's corporate clients, and procedures for addressing any deficiencies in those processes that could result in increased risk exposure for the institution;
- depending on the risk assessment for particular transactions, enhanced review of the overall customer relationship that considers the entire consolidated organization, so that risks are identified and managed on a comprehensive basis and not in silos; and
- procedures to ensure that business lines comply fully with company policy for consulting with or obtaining opinions from outside counsel on particular transactions or client relationships.

These measures provide a few examples of areas where professionals can and should assist their corporate clients. And it is clear that the timing is essential - almost as important as what to do is *when* to do it. Institutions cannot allow problems to develop to the point where regulators or law enforcement must identify them. Similarly, legal professionals should be proactive, informed, and engaged, and

should not confine themselves to a responsive role of addressing problems once they have progressed to a very serious stage.

Conclusion

In today's environment, regulators, lawmakers and shareholders are looking for providers of legal services to be vigilant on behalf of their clients and to ensure that clients receive the best possible assistance in meeting the standards for corporate governance, compliance, internal controls, and legal and reputational risk management. Your clients will be better served if your work reflects the highest professional standards and you take a proactive approach to help them avoid the financial, reputational and other penalties for failures in corporate governance.